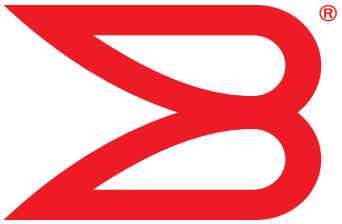
53-1001767-01
30 March 2010



Fabric OS

Message Reference

Supporting Fabric OS v6.4.0

BROCADE

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
Diagnostic and System Error Message Reference v3.0, v4.0	53-0000210-02	First release	March 2002
Diagnostic and System Error Message Reference v3.1.0	53-0000511-04	Major content reorganization	June 2003
Diagnostic and System Error Message Reference v4.1.0	54-0000515-02	Major content reorganization	June 2003
Diagnostic and System Error Message Reference v4.1.2	53-0000515-06	Minor editorial changes	October 2003
Diagnostic and System Error Message Reference v4.2.0	53-0000515-07	Add FW and PLATFORM messages	December 2003

Title	Publication number	Summary of changes	Date
Diagnostic and System Error Message Reference v4.2.0	53-0000515-08	Update software and hardware support	March 2004
Fabric OS System Error Message Reference Manual	53-0000515-09	Updated for v4.4.0, First RASLog release	August 2004
Fabric OS System Error Message Reference Manual	53-0000515-10	Added 22 ZONE messages	April 2005
Fabric OS System Error Message Reference Manual	53-0000515-11	Added FICU-1010, HAMK-1004, and PLAT-1001	July 2005
Fabric OS System Error Message Reference Manual	53-1000046-01	Added BM, FCR, IPS, FCIP, SEC, and ZONE messages	January 2006
Fabric OS System Error Message Reference Manual	53-1000046-02	Minor updates to a few messages.	June 2006
Fabric OS Message Reference	53-1000242-01	-Updated for Fabric OS v5.2.0: -changed doc title and number -Added the following new modules: IBPD, ICPD, ISCSI, ISNSCD. Added Audit messages: AUTH, CONF, HTTP, SEC, SNMP, SULB, ZONE -Updated Introduction chapter with AUDIT log information. -Updated chapter titles	September 2006
Fabric OS Message Reference	53-1000437-01	Updated for Fabric OS v5.3.0: -Added new chapters: AG, BKSW, IBD, IPAD, SAS. Revised and added new messages to: AUTH, CDR, CONF, EM, FABR, HAM, ISNS, ISW, PDM,SEC,TS, KTRC.SEC, TS. Revised/updated BL,BLL,FCPD, FICU,FW, HIL,LOG, SNMP, SULB,SWCH,SYSM, TRCE, ZOLB, ZONE. -Deleted USWD chapter. -Updated Introductory chapters. -Update throughout: rebranding, supported hardware, CLI changes.	June 2007
Fabric OS Message Reference	53-1000600-01	Updated for Fabric OS v6.0.0: -Added new chapters: C2, ESS, FICON -Added new messages to: AG, BL, BM, C2, FCIP, ISW, NS, PLAT, SS, HIL -Added Audit messages: SEC, SULB -Updated Introductory chapters.	October 2007
Fabric OS Message Reference	53-1000600-02	Updated for Fabric OS v6.1.0: -Revised and added new messages to: AG, BL, C2, EM, FABR, FCR, FCIP, FW, SEC, NS, PDM, PLAT, SULB, SWCH, ZONE, WEBD -Added new Audit chapter: FW -Added new Audit messages to: SEC -Updated Introductory chapters.	Jun 2008

Title	Publication number	Summary of changes	Date
Fabric OS Message Reference	53-1001116-01	Updated for Fabric OS v6.1.1_enc: -Revised and added new messages to AG -Added new chapters: CNM, CTAP, CVLC, CVLM, KAC, RKD, SPC, SPM -Added new Audit chapters: AG, FCIP, FICU, IPAD, PORT, SWCH, UCST -Updated Introductory chapters.	Aug 2008
Fabric OS Message Reference	53-1001157-01	Updated for Fabric OS v6.2.0: -Revised and added new messages to FSS, KSWD, CTAP, CNM, CVLM, EM, FABR, FCIP, FW, HIL, FCR, SEC, SWCH, UCST, ZONE -Added new chapters: CHASSIS, LFM, PMGR, TAPE --Updated Introductory chapters.	November 2008
Fabric OS Message Reference	53-1001338-01	Updated for Fabric OS v6.3.0: -Modified a message to BKSW, BL, BKSW, BLL, CDR, CEE CONFIG, CONF, EM, FCOE, FCPD, FCPH, FCR, FICON, FICU, FLOD, FSPF, FSSM, FW, HAM, ,HAMK, HIL, IPS, ISNS, L2SYS, MFIC, PDM, PLAT, PORT, RCS, RPCD, RTWR, SEC, SNMP, SWCH, TRCE, TRCK, WEBD, ZONE. -Added new messages to AG, AN, AUTH, BLS, C2, CDR, CEE, CONFIG, CHASSIS, CNM, CONF, CTAP, CVLC, CVLM, DAUTH, EM, FABR, FCIP, FCPH, FCR, FICON, FICU, FSPF, FSS, FW, HAM, HSL, KAC, KSWD, LANCE, LFM, MS, NS, NSM, PMGR, PORT, PSWP, RKD, SEC, SPC, SPM, SS, SULB, SWCH, TAPE, UCST, UPTH, XTUN, ZONE. -Added new chapters for LANCE, BLS, AN, CVLM, DAUTH, XTUN. -Updated Introductory chapters.	July 2009
Fabric OS Message Reference	53-1001338-02	Updated for Fabric OS v6.3.0 patch: -Modified a message to BL -Added new messages to AG, BL, and FCOE. -Added new chapters for Audit CNM, Audit CVLM, and Audit SPM.	November 2009
Fabric OS Message Reference	53-1001767-01	Updated for Fabric OS v6.4.0: -Modified messages to FICU and FW -Deleted a messages to BL, FCOE and FW -Added new messages to AG, AN, AUTH, BL, C2, CNM, CONF, CVLC, CVLM, FABR, FICU, FW, HAM, HIL, MQ, MS, MSTP, NS, NSM, ONM, PS, PSWP, RKD, SEC, SPM, SS, SSM, SULB, SWCH and ZONE. -Updated Introductory chapters.	March 2010

Contents

Chapter 22 EM System Messages

Chapter 90 SEC System Messages

Chapter 94 SPM System Messages

About This Document

In this chapter

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible.

The document contains the following components:

- Chapter 1, "Introduction To System Messages" provides basic information on system messages.
- Chapters 2 through 131 provides message syntax, probable cause, recommended action, and severity for each of the system messages.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for 6.4.0, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release of Fabric OS:

- Brocade 300
- Brocade 4100
- Brocade 4900

- Brocade 5000
- Brocade 5100
- Brocade 5300
- Brocade 5410
- Brocade 5424
- Brocade 5450
- Brocade 5460
- Brocade 5470
- Brocade 5480
- Brocade 7500
- Brocade 7500E
- Brocade 7600
- Brocade 7800
- Brocade 8000
- Brocade 48000
- Brocade Encryption Switch
- Brocade DCX Backbone
- Brocade DCX-4S Backbone
- Brocade VA-40FC

What's new in this document

The following changes have been made since this document was last released:

- Information that was modified:
  - "FICU System Messages"
  - "FW System Messages"
- Information that was deleted:
  - "BL System Messages"
  - "FCOE System Messages"
  - "FW System Messages"
- Information that was added:
  - "AG System Messages"
  - "AN System Messages"
  - "AUDIT AN System Messages"
  - "AUTH System Messages"
  - "AUDIT AUTH System Messages"
  - "BL System Messages"
  - "C2 System Messages"

- "CNM System Messages"
- "AUDIT CNM System Messages"
- "CONF System Messages"
- "AUDIT CONF System Messages"
- "CVLC System Messages"
- "CVLM System Messages"
- "AUDIT CVLM System Messages"
- "FABR System Messages"
- "FICU System Messages"
- "AUDIT FICU System Messages"
- "FW System Messages"
- "HAM System Messages"
- "HIL System Messages"
- "MQ System Messages"
- "MS System Messages"
- "MSTP System Messages"
- "NS System Messages"
- "NSM System Messages"
- "ONM System Messages"
- "PS System Messages"
- "RKD System Messages"
- "SEC System Messages"
- "AUDIT SEC System Messages"
- "SPM System Messages"
- "AUDIT SPM System Messages"
- "SS System Messages"
- "SSM System Messages"
- "SULB System Messages"
- "AUDIT SULB System Messages"
- "SWCH System Messages"
- "ZONE System Messages"

For further information about new features and documentation updates for this release, refer to the release notes.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
code text	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Command syntax conventions

Command syntax in this manual follows these conventions:

command	Commands are printed in bold.
--option, option	Command options are printed in bold.
-**argument,** arg	Arguments.
[ ]	Optional element.
variable	Variables are printed in italics. In the help pages, values are underlined or enclosed in angled brackets < >.
...	Repeat the previous element, for example “member[;member...]”
value	Fixed values following arguments are printed in plain font. For example, **--show** WWN
|	Boolean. Elements are exclusive. Example: **--show -mode** egress | ingress

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER

A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Key terms

For definitions specific to Brocade and Fibre Channel, see the *Brocade Glossary*.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Windows, Windows NT, Internet Explorer
Red Hat, Inc.	Red Hat, Red Hat Network, Maximum RPM, Linux Undercover

Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade resources

To get up-to-the-minute information, go to http://my.brocade.com and register at no cost for a user ID and password.

White papers, online demonstrations, and data sheets are available through the Brocade website at:

http://www.brocade.com/products-solutions/products/index.page

For additional Brocade documentation, visit the Brocade website:

http://www.brocade.com

Release notes are available on the MyBrocade website and are also bundled with the Fabric OS firmware.

Other industry resources

For additional resource information, visit the Technical Committee T11 website. This website provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association website:

http://www.fibrechannel.org

Getting technical help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. General Information
   - Switch model
   - Switch operating system version
   - Software name and software version, if applicable
   - Error numbers and messages received
   - **supportSave** command output
   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - syslog message logs
2. Switch Serial Number

   The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below.

   The serial number label is located as follows:

   - Brocade 300, 4100, 4900, 5100, 5300, 7500, 7800, 8000, and Brocade Encryption Switch—On the switch ID pull-out tab located inside the chassis on the port side on the left

- Brocade 5000—On the switch ID pull-out tab located on the bottom of the port side of the switch
- Brocade 7600—On the bottom of the chassis
- Brocade 48000—Inside the chassis next to the power supply bays
- Brocade DCX—On the bottom right on the port side of the chassis
- Brocade DCX-4S—On the bottom right on the port side of the chassis, directly above the cable management comb.
- World Wide Name (WWN)
- Use the **licenseIdShow** command to display the WWN of the chassis.
- If you cannot use the **licenseIdShow** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the Brocade DCX. For the Brocade DCX, access the numbers on the WWN cards by removing the Brocade logo plate at the top of the nonport side of the chassis.

Document feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

1 Introduction To System Messages

In this chapter

Overview of System Messages

This guide supports Fabric OS v6.4.0 and documents system messages that can help you diagnose and fix problems with a switch or fabric. The messages are organized first by event type, reliability, availability, and serviceability log (RASLog) or AUDIT, and then alphabetically by module name. A *module* is a subsystem in the Fabric OS. Each module generates a set of numbered messages. For each message, this guide provides message text, probable cause, recommended action, and severity level. There may be more than one cause and more than one recommended action for any given message. This guide discusses the most probable cause and typical action recommended.

This chapter provides an introduction to system messages. The Fabric OS maintains an internal system message log of all messages. All messages are tagged by type as either RASLog system error messages, Audit messages, or both. RASLog error messages are primarily designed to indicate and log abnormal, error-related events, whereas Audit messages record events such as login failures, zone, or configuration changes. Fabric OS supports a different methodology for storing and accessing each type of message.

System Error Message Logging

The RASLog service generates and stores messages related to abnormal or erroneous system behavior. It includes the following features:

- All RASLog error messages are saved to nonvolatile storage by default.
- The system error message log can save a maximum of 1024 messages in random access memory (RAM).
- The system message log is implemented as a circular buffer. When more than maximum entries are added to the log file, old entries are overwritten by new entries.
- Messages are numbered sequentially from 1 to 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.
- By default, the **errDump** and **errShow** commands display all of the system error messages.

- Trace dump, first-time failure detection capture (FFDC), and core dump files can be uploaded to the FTP server using the **supportSave** command.
- It is recommended to configure the **syslogd** facility as a management tool for error logs. This is particularly important for dual-domain switches because the **syslogd** facility saves messages from two logical switches as a single file and in sequential order. See "System Logging Daemon (syslogd)" on page 3 for more information.

Event Auditing

Event auditing is designed to support post-event audits and problem determination based on high-frequency events of certain types such as security violations, zoning configuration changes, firmware downloads, and certain types of fabric events. Fabric OS versions earlier than v5.2.0 generated a subset of messages flagged as AUDIT in the RASLog to identify some of this type of output in addition to error log messages. In Fabric OS v5.2.0 and later, messages flagged as AUDIT are no longer saved in the switch's error logs. Instead, the switch can be configured to stream Audit messages to the switch console and to forward the messages to specified syslog servers. There is no limit to the number of audit events.

For any given event, AUDIT messages capture the following information:

- User Name - The name of the user who triggered the action.
- User Role - The access level of the user, such as, root or admin.
- Event Name - The name of the event that occurred.
- Status - The status of the event that occurred: success or failure.
- Event Info - Information about the event.

The five event classes described in the following table can be audited.

TABLE 1

Operand	Event Class	Description
1	Zone	You can audit zone event configuration changes, but not the actual values that were changed. For example, you may receive a message that states "Zone configuration has changed," but the message does not display the actual values that were changed.
2	Security	You can audit any user-initiated security event for all management interfaces. For events that have an impact on the entire fabric, an audit is only generated for the switch from which the event was initiated.
3	Configuration	You can audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.
4	Firmware	You can audit configuration downloads of existing SNMP configuration parameters. Configuration uploads are not audited.
5	Fabric	You can audit Administration Domain related changes.

Fabric OS v6.4.0 generates component-specific Audit messages see "Audit Log Messages".

Event auditing is a configurable feature, set to off by default. You must enable event auditing by configuring the syslog daemon to send the events to a configured remote host using the **syslogIpAdd** command. You can set up filters to screen out particular classes of events using the **auditCfg** command (the classes include zone, security, configuration, firmware, and fabric). The

defined set of Audit messages are sent to the configured remote host in the Audit message format, so that they are easily distinguishable from other syslog events that might occur in the network. For details on how to configure event auditing, see "Viewing and Configuring System Message Logs" on page 4.

System Logging Daemon (syslogd)

The system logging daemon (**syslogd**) is a process on UNIX, Linux, and some Windows systems that reads and logs messages as specified by the system administrator.

Fabric OS can be configured to use a UNIX-style **syslogd** process to forward system events and error messages to log files on a remote host system. The host system can be running UNIX, Linux, or any other operating system that supports the standard **syslogd** functionality. Configuring for **syslogd** involves configuring the host, enabling **syslogd** on the Brocade model, and, optionally, setting the facility level.

For the *Brocade DCX, 24000 and 48000*, each CP has a unique error log, depending on which CP was active when that message was reported. To fully understand message logging on the *Brocade 24000 and 48000* you should enable the system logging daemon, because the logs on the host computer are maintained in a single merged file for both CPs and are in sequential order. Otherwise, you must examine the error logs in both CPs, particularly for events such as **firmwareDownload** or **haFailover**, for which the active CP changes.

For the *Brocade DCX, 24000 and 48000*, any security violations that occur through Telnet, HTTP, or serial connections are not propagated between CPs. Security violations on the active CP are not propagated to the standby CP counters in the event of a failover, nor do security violations on the standby CP get propagated to the active CP counters.

For information on configuring **syslogd** functionality, refer to the *Fabric OS Administrator's Guide*.

System Console

The system console displays messages only through the serial port. If you log in to a switch through the Ethernet port or modem port, you will not receive system console messages.

The system console displays system messages, Audit messages (if enabled) and panic dump messages. These messages are mirrored to the system console; they are always saved in one of the system logs.

You can filter messages that appear on the system console by severity using the **errFilterSet** command. All messages are still sent to the system message log and syslog (if enabled).

Port Logs

The Fabric OS maintains an internal log of all port activity. Each switch or logical switch maintains a log file for each port. Port logs are circular buffers that can save up to 8000 entries per logical switch. When the log is full, the newest log entries overwrite the oldest log entries. Port logs capture switch-to-device, device-to-switch, switch-to-switch, some device A-to-device B, and control information. Port logs are not persistent and are lost over power cycles and reboots.

Run the **portLogShow** command to display the port logs for a particular port.

Run the **portLogEventShow** command to display the specific events reported for each port.

Refer to the *Fabric OS Administrator's Guide* for information on interpreting results of the **portLogDump** command.

Port log functionality is completely separate from the system message log. Port logs are typically used to troubleshoot device connections.

Viewing and Configuring System Message Logs

This section provides information on viewing and configuring system message logs, including.

- Viewing System Messages from Web Tools
- Dumping System Messages
- Viewing System Messages One Message at a Time
- Clearing the System Message Log
- Configuring Event Auditing

The procedures are valid for the Brocade DCX, 200E, 3016, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, AP 76000, 24000, and 48000.

Table 2 describes commands that you can use to view or configure the system message logs. Most commands require admin access level. For detailed information on required access levels and commands, refer to the *Fabric OS Command Reference*.

TABLE 2 Commands for Viewing or Configuring the System Parameters and Logs

Command	Description
agtCfgDefault	Resets the SNMP recipients to default values.
agtCfgSet	Modifies the SNMP agent configuration.
agtCfgShow	Displays the current SNMP agent configuration.
auditCfg	Configures the audit message log.
auditShow	Modifies and displays audit log filter configuration.
diagPost	Sets or displays diagnostic POST (Power-On Self-Test) configuration.
errClear	Clears all error log messages for all switch instances on this control processor (CP).
errDelimterSet	Sets the error log start and end delimiter for messages pushed to the console.
errDump	Displays the entire error log, without page breaks. Use the **-r** option to show the messages in reverse order, from newest to oldest.
errFilterSet	Sets an error severity filter for the system console.
errShow	Displays the entire error log, with page breaks. Use the **-r** option to show the messages in reverse order, from newest to oldest.
pdShow	Displays the contents of the panic dump and core dump files.
portErrShow	Displays the port error summary.
portLogClear	Clears the port log. If the port log is disabled, this command enables it.
portLogDisable	Disables the port log facility.
portLogDump	Displays the port log, without page breaks.
portLogDumpPort	Displays the port log of the specified port, without page breaks.
portLogEventShow	Displays which port log events are currently being reported.
portLoginShow	Displays port logins.
portLogPdisc	Sets or clears the debug pdisc_flag.
portLogReset	Enables the port log facility.
portLogResize	Resizes the port log to the specified number of entries.
portLogShow	Displays the port log, with page breaks.
portLogShowPort	Displays the port log of specified port, with page breaks.
portLogTypeDisable	Disables an event from reporting to the port log. Port log events are described by the **portLogEventShow** command.
portLogTypeEnable	Enables an event to report to the port log. Port log events are described by the **portLogEventShow** command.
setVerbose	Sets the verbose level of a particular module within the Fabric OS.
supportFtp	Sets, clears, or displays support FTP parameters or a time interval to check the FTP server.

TABLE 2 Commands for Viewing or Configuring the System Parameters and Logs (Continued)

Command	Description
supportFfdc	Enables and disables FFDC (first failure data capture).
supportSave	Collects RASLog, trace files, and **supportShow** (active CP only) information for the local CP and then transfers the files to an FTP server. The operation can take several minutes.
supportShow	Executes a list of diagnostic and error display commands. This output is used by your switch service provider to diagnose and correct problems with the switch. The output from this command is very long.
syslogDIpAdd	Adds an IP address as a recipient of system messages.
syslogDIpRemove	Removes an IP address as a recipient of system messages.
syslogDIpShow	Views the currently configured IP addresses that are recipients of system messages.
syslogdFacility	Changes the **syslogd** facility.
systemVerification	Use this command to run a comprehensive system wide test of all switches in a system. It will initiate a burnin run on all switches within the current system. Note that any reference seen to slot 0 is a reference to the blade within the switch platform, e.g.,Brocade 7500 and AP7600 contain FR4-18i and FA4-18 blades respectively.
traceDump	Displays, initiates, or removes a Fabric OS module trace dump.
traceTrig	Sets, removes, or displays trace triggers.

Viewing System Messages from Web Tools

To view the system message log for a switch from Web Tools:

1. Launch Web Tools.
2. Select the desired switch from the Fabric Tree. The Switch View displays.
3. Click the **Switch Events** button. A Switch Events Report displays.
4. View the switch events and messages.

In dual-domain switches, an Event button exists for each logical switch. Only messages relating to that switch (and chassis) will be displayed.

Dumping System Messages

To display the system message log, with no page breaks:

1. Log in to the switch as admin.
2. Enter the **errDump** command at the command line:

```
switch:admin> errDump
Version: 5.0.1
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in sync

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out of sync
```

```
2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port media
incompatible. Reason: Configured port speed.

2004/07/28-17:04:54, [FABR-1001], 4,, WARNING, switch, port 4, ELP rejected by
the other switch

2004/07/28-17:05:06, [FW-1050], 5,, WARNING, switch, Sfp Supply Voltage 0, is
below low boundary(High=3600, Low=3150). Current value is 0 mV.

switch:admin>
```

Viewing System Messages One Message at a Time

To display the system message log one message at a time:

1. Log in to the switch as admin.
2. At the command line, enter the **errShow** command:

```
switch:admin> errShow
Version: 5.0.1
2004/07/28-17:04:59, [FSSM-1002], 1,, INFO, switch, HA State is in sync

Type <CR> to continue, Q<CR> to stop:

2004/07/28-17:04:59, [FSSM-1003], 2,, WARNING, switch, HA State out of sync

Type <CR> to continue, Q<CR> to stop:

2004/07/28-17:04:51, [EM-1055], 3,, WARNING, switch, Media 27: Port media
incompatible
e. Reason: Configured port speed.

Type <CR> to continue, Q<CR> to stop:
```

Clearing the System Message Log

To clear the system message log for a particular switch instance:

1. Log in to the switch as admin.
2. Use the **errClear** command to clear all messages from memory.

NOTE

For products that have a single processor, all error log messages are cleared. For products that have multiple processors, this command only clears the error logs of the processor it is executed from.

Configuring Event Auditing

To configure event auditing:

1. Configure the event classes you wish to audit:

```
switch:admin> auditcfg --class 1,2,3,4,5
Audit filter is configured.
```

2. Verify the configuration:

```
switch:admin> auditcfg --show
Audit filter is enabled.
1-ZONE
2-SECURITY
3-CONFIGURATION
4-FIRMWARE
5-FABRIC
```

3. Enable the audit feature:

```
switch:admin> auditcfg --enable
Audit filter is enabled.
```

4. Configure up to six syslog servers to receive the audit events that will be generated through syslog (procedure will vary depending on server type).
5. Configure syslog on the switch to point to the configured servers' IP addresses.

```
switch:admin> syslogdipadd 10.128.128.160
```

6. Verify the switch's syslog configuration:

```
switch:admin> syslogdipshow
syslog.1        192.168.163.234
syslog.2        10.128.128.160
```

Reading a RAS System Message

This section provides information about reading system messages.

The following example shows the format of the RAS system error message:

```
<timestamp>, [<Event ID>], <Sequence Number>, <Flags>,<Severity>,<Switch
name>, <Event-specific information>
```

The following example shows a sample message from the error log:

```
2009/02/10-14:18:04, [SS-1000], 88, SLOT 6 | FFDC | CHASSIS, INFO, ESNSVT_DCX,
supportSave has uploaded support information to the host with IP address
168.159.16.128

2009/02/10-14:13:34, [SS-1001], 87, SLOT 6/1 | FFDC | CHASSIS, WARNING,
ESNSVT_DCX, supportSave's upload operation to host IP address aborted

2009/02/10-15:44:51, [SEC-1203], 89, SLOT 6 | FFDC | FID 128, INFO, ESNSVT_DCX,
Login information: Login successful via TELNET/SSH/RSH. IP Addr:168.159.16.128
```

The fields in the error message are described in Table 3.:

TABLE 3 System Message Field Description

Example	Variable Name	Description
2004/07/22-10:12:33	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem supports an internationalized timestamp format base on the "LOCAL" setting.

TABLE 3 System Message Field Description (Continued)

Example	Variable Name	Description
[EM-1031]	Message Module and Message Number	The message module and number. These values uniquely identify each message in the Fabric OS and reference the cause and actions recommended in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.
4	Sequence Number	The error message position in the log. When a new message is added to the log, this number is incremented by 1. When this message reaches the last position in the error log and becomes the oldest message in the log, it is deleted when a new message is added. The message sequence number starts at 1 after a **firmwareDownload** and will increase up to a value of 2,147,483,647 (0x7fffffff). The sequence number will continue to increase beyond the storage limit of 1024 messages. The sequence number can be reset to 1 using the **errClear** command. The sequence number is persistent across power cycles and switch reboots.
<NULL> (blank)	Audit and/or FFDC/SLOT/CHASSIS/FID Flags	For most messages, this field contains a space character (null value) indicating that the message is neither an AUDIT or FFDC message. Messages may contain the following values: AUDIT indicates that this message is for a security issue. FFDC indicates that additional first failure data capture information has also been generated for this event. FID is the Fabric ID that can range from 0 to 128. FID 128 means the message was generated by the default switch instance. CHASSIS is the message that was generated by the chassis instance. SLOT number indicates the message was generated from slot # blade main CPU. SLOT #/1 indicates the message was generated from slot # blade Co-CPU. AUDIT:FFDC indicates that the message is for a security issue and additional FFDC information has been generated.
ERROR	Severity Level	The severity of the error: 1 = Critical 2 = Error 3 = Warning 4 = Info
switchname	Switch name or chassis name, depending on the action; for example, high-availability (HA) messages typically show the chassis name, and login failures show the logical switch name.	The defined switch name or the chassis name of the switch. This value is truncated if it exceeds 16 characters in length. Run either the **chassisName** command to name the chassis or the **switchName** command to rename the logical switch.
Slot 7 ejector not closed	Error Description	A text string explaining the error encountered and providing parameters supplied by the software at runtime.

Audit Event Messages

Compared to RASLog error messages, messages flagged as AUDIT provide additional user and system-related information of interest for post event auditing and problem determination.

Audit event message format:

```
AUDIT, <timestamp>, [<Event ID>], <Severity>, <Event Class>, <User
ID>/<Role>/<IP address>/<Interface>/<app name>. <Admin Domain>/<Switch name>,
<Reserved field for future expansion>, <Event-specific information>
```

The following is a sample audit event message:

```
AUDIT, 2005/12/10-09:54:03, [SEC-1000], WARNING, SECURITY,
JohnSmith/root/192.168.132.10/Telnet/CLI, Domain A/JohnsSwitch, , Incorrect
password during login attempt.
```

The fields in the error message are described in Table 4.

TABLE 4 Audit Message Field Description

Example	Variable Name	Description
AUDIT	Audit flag	Identifies the message as an Audit message.
2005/12/10-09:54:03	Date and Time Stamp	The system time (UTC) when the message was generated on the switch. The RASLog subsystem will support an internationalized timestamp format base on the “LOCAL” setting.
[SEC-1000]	Message Module and Message Number	The message module and number. These values uniquely identify each message in the Fabric OS and reference the cause and actions recommended in this manual. Note that not all message numbers are used; there can be gaps in the numeric message sequence.
WARNING	Severity Level	The severity of the error: 1 = Critical 2 = Error 3 = Warning 4 = Info
SECURITY	Event Class	The event class: Zone Security Configuration Firmware Fabric
JohnSmith	User ID	The user ID.
root	Role	The role of the user ID.
192.168.132.10	IP Address	The IP address.
Telnet	Interface	The interface being used.
CLI	Application Name	The application name being used on the interface.
Domain A	Admin Domain	The Admin Domain, if there is one.

TABLE 4 Audit Message Field Description (Continued)

Example	Variable Name	Description
`switchname`	Switch name or chassis name, depending on the action; for example, HA messages typically show the chassis name and login failures show the logical switch name.	The defined switch name or the chassis name of the switch. This value is truncated if it is over 16 characters in length. Run either the **chassisName** command to name the chassis or the **switchName** command to rename the logical switch.
`, ,`	Null	Reserved for future use.
`Slot 7 ejector not closed`	Error Description	A text string explaining the error encountered and providing parameters supplied by the software at runtime.

Message Severity Levels

There are four levels of severity for messages, ranging from Critical (1) to Info (4). In general, the definitions are wide ranging and are to be used as general guidelines for troubleshooting. For all cases, you should look at each specific error message description thoroughly before taking action. System messages have the following severity levels.

1 = CRITICAL	Critical-level messages indicate that the software has detected serious problems that will cause a partial or complete failure of a subsystem if not corrected immediately; for example, a power supply failure or rise in temperature must receive immediate attention.
2 = ERROR	Error-level messages represent an error condition that does not impact overall system functionality significantly. For example, error-level messages might indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
3 = WARNING	Warning-level messages highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode unless the failed power supply is replaced or fixed.
4 = INFO	Info-level messages report the current non-error status of the system components: for example, detecting online and offline status of a fabric port.

Responding to a System Message

This section provides procedures on gathering information on system messages, including:

- Looking Up a System Message
- Gathering Information About the Problem
- Support
- Panic Dump and Core Dump Files
- Trace Dumps
- supportSave Command

Looking Up a System Message

Error messages in this manual are arranged alphabetically. To look up an error message, copy down the module (see Table 5 on page 14) and the error code and compare this with the Table of Contents to determine the location of the information for that error message.

The following information is provided for each message:

- Module and code name for the error
- Message text
- Probable cause
- Recommended action
- Message severity

Gathering Information About the Problem

Common steps and questions to ask yourself when troubleshooting a system message are as follows:

1. What is the current Fabric OS level?
2. What is the switch hardware version?
3. Is the switch operational?
4. Assess impact and urgency:
   - Is the switch down?
   - Is it a standalone switch?
   - How large is the fabric?
   - Is the fabric redundant?
5. Run the **errDump** command on each logical switch.
6. Run the **supportFtp** command (as needed) to set up automatic FTP transfers, and then run the **supportSave** command.
7. Document the sequence of events by answering the following questions:
   - What happened just prior to the problem?
   - Is the problem repeatable?
   - If so, what are the steps to produce the problem?
   - What configuration was in place when the problem occurred?
8. Did a failover occur?
9. Was security enabled?
10. Was POST enabled?
11. Are serial port (console) logs available?
12. Which CP was master? (only applicable to the Brocade DCX, 12000, 24000, or 48000)
13. What and when were the last actions or changes made to the system?

Support

Fabric OS creates a number of files that can help support personnel troubleshoot and diagnose a problem. This section describes those files and how to access and/or save the information for support personnel.

Panic Dump and Core Dump Files

The Fabric OS creates panic dump files and core files when there are problems in the Fabric OS kernel. You can view panic dump files using the **pdShow** command. These files can build up in the kernel partition (typically because of failovers) and might need to be periodically deleted or downloaded using the **supportSave** command.

The software watchdog process (SWD) is responsible for monitoring daemons critical to the function of a healthy switch. The SWD holds a list of critical daemons that ping the SWD periodically at a predetermined interval defined for each daemon. The ping interval is set at 133 seconds, with the exception of the Fabric Watch daemon and the IP storage demon, which ping the SWD every 333 seconds. (For a complete listing of daemons, see the KSWD entry in Table 5.)

If a daemon fails to ping the SWD within the defined interval, or if the daemon terminates unexpectedly, then the SWD dumps information to the panic dump files, which helps to diagnose the root cause of the unexpected failure.

Run the **pdShow** command to view these files or the **supportSave** command to send them to a host workstation using FTP. The panic dump files and core files are intended for support personnel use only.

Trace Dumps

The Fabric OS produces trace dumps when problems are encountered within Fabric OS modules. The Fabric OS trace dump files are intended for support personnel use only. You can use the **supportSave** or **supportFTP** commands to collect trace dump files to a specified remote location to provide to support when requested.

supportSave Command

The **supportSave** command can be used to send the output of the system messages (RASLog), the trace files, and the output of the **supportShow** command to an off-switch storage location through FTP. Prior to running the **supportSave** command, you can optionally set up the FTP parameters using the **supportFtp** command. The **supportShow** command runs a large number of dump and show commands to provide a global output of the status of the switch. Refer to the *Fabric OS Command Reference* for more information on these commands.

System Module Descriptions

NOTE

Any reference seen in a system message to slot 0 is a reference to the blade within the switch platform, for example: Brocade DCC contains FC8-48, FC9-32, and FC8-16 blades.

Table 5 provides a summary of the system modules for which messages are documented in this reference guide; the system modules are listed alphabetically by name.

TABLE 5 System Module Descriptions

System Module	Description
AG	Access Gateway allows multiple hosts (or HBAs) to access the fabric using fewer physical ports. Access Gateway mode transforms the Brocade switches as well as embedded switches into a device management tool that is compatible with different types of fabrics, including Brocade-, Cisco-, and McDATA-based fabrics.
AN	Error or warning messages from the Bottleneck Detection module, including notification of detected bottlenecks
ANV	ANV error messages indicate problems with the driver that deal with the ENET ASICs on the Fabric OS. They could be either software or hardware-related errors.
AUTH	Authentication error messages indicate problems with the authentication module of the Fabric OS.
BKSW	Messages generated by the Blade Fabric OS kernel software watch dog module.
BL	Blade error messages are a result of faulty hardware, transient out-of-memory conditions, application specific integrated circuit (ASIC) errors, or inconsistencies in the software state between a blade and the EM (environment monitor) module.
BLL	Bloom is the name of the application specific integrated circuit (ASIC) used as the building block for third-generation hardware platforms.
BLS	Fibre Channel over IP port configuration message over Spike and Striker Blade.
BM	Blade management error messages are a result of autoleveling firmware upgrades performed by the control processor (CP).
C2	Condor2 error messages indicate problems with the Condor2 ASIC driver module of the Fabric OS.
CDR	Condor application specific integrated circuit (ASIC) driver error messages.
CEE CONFIG	CEEConfig error messages indicate problems with the Converged Enhanced Ethernet Configuration module of the Fabric OS.
CER	This is the core edge routing module on the Brocade director platforms.
CHASSIS	Error messages reporting the problems in the management of the blades in the different slots of the chassis.
CNM	CNM (Cluster Node Manager) is a software daemon module of the Fabric OS. The messages from CNM are either problems encountered by CNM, warnings or information to inform the user of events.
CONF	Status messages for **configUpload** and **configDownload** operations.
CTAP	A user-space daemon that forwards non-performance-critical messages from the TAPE driver to the CVLC and Security Processor (SP), and vice versa. This module also maintains a cache of recently acquired keys, reducing requests to the key vault itself.
CVLC	CVLC (Crypto Virtual LUN Controller) is a software module running on BFOS. The messages of CVLC are either problems encountered by CVLC, warnings to alert user, or informative to user.
CVLM	CVLM (Crypto Virtual LUN Manager) is a software module of the Fabric OS. The messages of CVLM are either problems encountered by CVLM, warnings to alert the user, or informative to the user.
DAUTH	DAUTH error messages indicate problems with the 802.1x authentication module of the Fabric OS.

TABLE 5 System Module Descriptions (Continued)

System Module	Description
EM	The environmental monitor (EM) manages and monitors the various field replaceable units (FRUs), including the port cards, control processor (CP) blades, blower assemblies, power supplies, and world wide name (WWN) cards. EM controls the state of the FRUs during system startup, hot-plug sequences, and fault recovery. EM provides access to and monitors the sensor and status data from the FRUs and maintains the integrity of the system using the environmental and power policies. EM reflects system status by way of CLI commands, system light emitting diodes (LEDs), and status and alarm messages. EM also manages some component-related data.
ESS	ESS (Exchange Switch Support) error messages indicate problems with the ESS module of the Fabric OS. ESS is an SW_ILS mechanism utilized by switches to exchange vendor and support information.
ESWCH	ESWCH error messages indicate problems with the Ethernet switch module of Fabric OS.
EVMD	This is the event management module.
FABR	FABRIC refers to a network of Fibre Channel switches. The FABRIC error messages come from the fabric daemon. The fabric daemon follows the FC-SW-3 standard for the fabric initialization process, such as determining the E_Ports, assigning unique domain IDs to switches, creating a spanning tree, throttling the trunking process, and distributing the domain and alias lists to all switches in the fabric.
FABS	Fabric OS system driver module.
FBC	Firmware blade compatibility errors with control processor (CP).
FCIP	Fibre Channel over IP port configuration messages over Sprint and Marathon Blade.
FCMC	Fibre Channel miscellaneous messages relate to problems with the physical layer used to send Fibre Channel traffic to and from the switch.
FCOE	FCoE error messages indicate problems with the FCoE module of the Fabric OS.
FCPD	The Fibre Channel Protocol daemon is responsible for probing the devices attached to the loop port. Probing is a process the switch uses to find the devices attached to the loop ports and to update the Name Server with the information.
FCPH	Fibre Channel Physical Layer is used to send Fibre Channel traffic to and from the switch.
FCR	Fibre Channel router-related traffic and activity on the fabric or backend fabric.
FICON	The FICN-1xxx and FICN-5yyy messages are generated during FICON emulation processing on an FCIP Tunnel.
FICON CUP	FICU-#### messages indicate that something has occurred which affects the control unit port (CUP) for the switch/director. These messages can mean anything from configuration-related failures to internal software errors.
FICU	The FICON-CUP daemon handles communication with fibre connectivity (FICON) on IBM FICON storage devices. Errors to this module are usually initiation errors or indications that FICON-CUP prerequisites have not been met, such as a license key, core process ID (PID), and secure mode on the fabric.
FKLB	Fabric OS I/O kernel library module.
FLOD	FLOD is a part of the fabric shortest path first (FSPF) protocol that handles synchronization of the link state database (LSDB) and propagation of the link state records (LSRs).
FSPF	Fabric shortest path first (FSPF) is a link state routing protocol that is used to determine how frames should be routed. These messages are about protocol errors.

TABLE 5 System Module Descriptions (Continued)

System Module	Description
FSS	The Fabric OS state synchronization framework provides facilities by which the active control processor (CP) can synchronize with the standby CP, enabling the standby CP to take control of the switch nondisruptively during failures and software upgrades. These facilities include version negotiation, state information transfer, and internal synchronization functions, enabling the transition from standby to active operation. FSS is defined both as a component and a service. A *component* is a module in the Fabric OS, implementing a related set of functionality. A *service* is a collection of components grouped together to achieve a modular software architecture.
FSSM	The Fabric OS state synchronization management module is defined both as a component and a service. A component is a module in Fabric OS implementing a related set of functionality. A service is a collection of components grouped together to achieve a modular software architecture.
FW	FW is the Fabric Watch module. This module monitors thresholds for many switch subsystems: for example, temperature, voltage, fan speed, and switch status. Any changes that cross a specified threshold are reported to the system message log.
HAM	HAM is a user space daemon responsible for high availability management.
HAMK	This is the kernel module for the high availability management (HAM) daemon.
HIL	Hardware independent layer.
HLO	HLO is a part of the fabric shortest path first (FSPF) protocol that handles the HELLO protocol between adjacent switches. The HELLO protocol is used to establish connectivity with a neighbor switch, to establish the identity of the neighbor switch, and to exchange FSPF parameters and capabilities.
HMON	Health monitor.
HSL	HSL error messages indicate problems with the Hardware Subsystem Layer of the Fabric OS.
HTTP	HTTP error messages.
IBD	This raslog generates messages related to port restart failure.
IBPD	IBPD stands for iSCSI gateway daemon on a blade processor (BP). It manages iSCSI initiator access control, session authentication, and session/connection statistics.
ICPD	ICPD stands for iSCSI gateway daemon on a control processor (CP). It manages iSCSI configurations such as CHAP, VT/LUN, DD/DDSet and portal configurations, and statistics such as iSCSI session/connection information. Moreover, ICPD distributes iSCSI configurations not only switch wide, but also fabric wide. It keeps track iSCSI VT status and updates VT status to BP.
IPAD	System messages generated by the IP admin demon.
IPS	Fibre Channel over IP license, tunneling, and port-related messages.
ISCS	The ISCS module is the FabOS component that performs system-level control of the iSCSI Gateways. Its functions include: initialization, message delivery from iSCSI protocol clients, system error monitoring, and fault recovery.
ISNS	ISNS server and client status messages.
KAC	KAC error messages indicate problems associated with Fabric OS and the external key vaults.

TABLE 5 System Module Descriptions (Continued)

System Module	Description
KSWD	The kernel software watchdog (KSWD) watches daemons for unexpected terminations and "hang" conditions and informs the HAM module to take corrective actions such as failover or reboot. The following daemons are monitored by KSWD: • Access Gateway daemon (agd) • Alias Server (asd) • ARR daemon (arrd) • Authentication daemon (authd) • Blade Manager (bmd) • Common Access Layer (cald) • Diagnostics daemon (diagd) • Environment Monitor (emd) • EVM daemon (evmd) • Exchange Service Support daemon (essd) • FA-API rpc daemon (rpcd) • Fabric daemon (fabricd) • Fabric Watch daemon (fwd) • FCPD daemon (fcpd) • FDMI daemon (fdmid) • FICON CUP daemon (ficud) • FSPF daemon (fspfd) • Inter-fabric Routing daemon (iswitchd) • IP Storage Daemon (ipsd) • iSCSI daemon on CP (icpd) • iSNS client daemon on CP (isnscd) • Management Server daemon (msd) • Name Server Daemon (nsd) • PDM daemon (pdmd) • PS daemon (psd) • RASLOG daemon (raslogd) • RSC daemon (rcsd) • SAS CP Daemon (scpd) • Security daemon (secd) • SNMP daemon (snmpd) • Time Service daemon (tsd) • TRACE daemon (traced) • Track Changes daemon (trackd) • Web tools daemon (webd)
KTRC	Kernel RAS trace module.
L2SYS	L2sys error messages indicate problems with the L2 System manager that controls the Layer 2 forwarding engine and controls the learning/aging/forwarding functionality.
LACP	LACP error messages indicate problems with the Link Aggregation Control Protocol module of the Fabric OS.
LANCE	LANCE error messages indicate problems with the LANCE module of the Fabric OS.
LFM	LFM error messages indicate problems with the logical fabric manager module that is responsible for making a logical switch use XISLs. This involves creating and managing LISLs in a logical fabric.
LOG	RASLog subsystem.
LSDB	The link state database is a part of the FSPF protocol that maintains records on the status of port links. This database is used to route frames.

TABLE 5 System Module Descriptions (Continued)

System Module	Description
MFIC	MS-FICON messages relate to Fibre Connection (FICON) installations. Fibre Connection control unit port (FICON-CUP) messages are displayed under the FICU module.
MPTH	Multicast path uses the shortest path first (SPF) algorithm to dynamically compute a broadcast tree.
MQ	Message queues are used for interprocess communication. Message queues allow many messages, each of variable length, to be queued. Any process or interrupt service routine (ISR) can write messages to a message queue. Any process can read messages from a message queue.
MS	The Management Service enables the user to obtain information about the Fibre Channel fabric topology and attributes by providing a single management access point. MS provides for both monitoring and control of the following areas: **Fabric Configuration Server**. Provides for the configuration management of the fabric. **Unzoned Name Server**. Provides access to Name Server information that is not subject to zone constraints. **Fabric Zone Server**. Provides access to and control of zone information.
MSTP	MSTP error messages indicate problems with Multiple Spanning Tree Protocol modules of the Fabric OS.
NBFS	NBFSM is a part of the fabric shortest path first (FSPF) protocol that handles a neighboring or adjacent switch's finite state machine (FSM). Input to the FSM changes the local switch from one state to another, based on specific events. For example, when two switches are connected to each other using an ISL (interswitch link) cable, they are in the Init state. After both switches receive HELLO messages, they move to the Database Exchange state, and so on. NBFSM states are Down (0), Init (1), Database Exchange (2), Database Acknowledge Wait (3), Database Wait (4), and Full (5).
NS	Indicates problems with the simple name server module.
NSM	NSM error messages indicate problems with the Interface Management and VLAN Management module of the Fabric OS.
ONM	ONM error messages indicate problems with the Operation, Administration and Maintenance module of the Fabric OS.
PDM	Parity data manager is a user space daemon responsible for the replication of persistent configuration files from the primary partition to the secondary partition and from the active CP blade to the standby CP blade.
PDTR	These messages indicate panic dump trace files have been created.
PLAT	This message indicates hardware problems.
PMGR	A group of messages relating to logical switch creation, deletion and configuration.
PORT	PORT error messages refer to the front-end user ports on the switch. Front-end user ports are directly accessible by users to connect end devices or connect to other switches.
PS	The performance server daemon measures the amount of traffic between end points or traffic with particular frame formats, such as SCSI frames, IP frames, and customer-defined frames.
PSWP	The portswap feature and associated commands generate these error messages.
RAS	First failure data capture (FFDC), informational message when FFDC events are logged to the FFDC log and size/roll over warning.

TABLE 5 System Module Descriptions (Continued)

System Module	Description
RCS	The reliable commit service daemon generates log entries when it receives a request from the zoning, security, or management server for passing data messages to switches in the fabric. RCS then requests reliable transport write and read (RTWR) to deliver the message. RCS also acts as a gatekeeper, limiting the number of outstanding requests for the Zoning, Security, or Management Server modules.
RKD	These messages are either error or informational messages pertaining to the Rekey daemon of the Fabric OS.
RMOND	RMOND messages are error or informational messages pertaining to the RMOND daemon.
RPCD	The remote procedure call daemon (RPCD) is used by Fabric Access for API-related tasks.
RTWR	The reliable transport write and read daemon helps deliver data messages either to specific switches in the fabric or to all of the switches in the fabric. For example, if some of the switches are not reachable or are offline, RTWR returns an “unreachable” message to the caller, allowing the caller to take the appropriate action. If a switch is not responding, RTWR retries 100 times.
SAS	Storage application services supporting director-class storage virtualization platform.
SCN	The internal state change notification daemon is used for state change notifications from the kernel to the daemons within Fabric OS
SEC	The security daemon generates security errors, warnings, or information during security-related data management or fabric merge operations. Administrators should watch for these messages, to distinguish between internal switch and fabric operation errors, and external attack.
SNMP	Simple Network Management Protocol is a universally supported low-level protocol that allows simple get, get next, and set requests to go to the switch (acting as an SNMP agent). It also allows the switch to send traps to the defined and configured management station. Brocade switches support six management entities that can be configured to receive these traps.
SPC	SPC messages indicate problems and informational updates associated with the security processor. These messages could be tiggered by the following three modules: Security processor controller, SP system controller and SP Keyapp.
SPM	Error messages indicating problems either with key or SP management.
SS	The **supportSave** command generates these error messages if problems are encountered.
SSM	SSM error messages indicate problems with the System Services Module of the Fabric OS.
SULB	The software upgrade library provides the **firmwareDownload** command capability, which enables firmware upgrades to both CP blades with a single command, as well as nondisruptive code load to all 4.x switches. These messages might display if there are any problems during the **firmwareDownload** procedure. Most messages are informational only and are generated even during successful firmware download. For additional information, refer to the *Fabric OS Administrator’s Guide*.
SWCH	These messages are generated by the switch driver module that manages a Fibre Channel switch instance.
SYSC	System controller is a daemon that starts up and shuts down all Fabric OS modules in the proper sequence.
SYSM	General system messages.
TAPE	A kernel-space driver that handles all I/O operations aimed at tape containers.
TRCE	RAS TRACE error messages.

TABLE 5 System Module Descriptions (Continued)

System Module	Description
TRCK	The track change feature tracks the following events: Turning on or off the track change feature CONFIG_CHANGE LOGIN LOGOUT FAILED_LOGIN If any of these events occur, a message is sent to the system message log. Additionally, if the SNMP trap option is enabled, an SNMP trap is also sent. For information on configuring the track change feature, refer to the *Fabric OS Command Reference* or the *Fabric OS Administrator's Guide*.
TS	Time Service provides fabric time-synchronization by synchronizing all clocks in the fabric to the clock time on the principal switch.
UCST	UCST is a part of the fabric shortest path first (FSPF) protocol that manages the Unicast routing table.
UPTH	UPATH is a part of the FSPF protocol that uses the SPF algorithm to dynamically compute a Unicast tree.
WEBD	Indicates problems with the Web Tools module.
XTUN	XTUN Messages are generated by the 7800/FX8-24 FCIP Tunnel implementation. These messages indicate status of FCIP Tunnels, FCIP Emulation Events for FCP traffic or FCIP Debug information (FTRACE buffer status changes).
ZEUS	Zeus error messages indicate problems with the Zeus driver module.
ZOLB	Indicates problems with the zone library module.
ZONE	The zone module messages indicate any problems associated with the zoning features, including commands associated with aliases, zones, and configurations.

Section

I

RASLog Messages

This section provides the RASLog messages, including:

Chapter

AG System Messages

2

AG-1001

Message `<timestamp>, [AG-1001], <sequence-number>,, ERROR, <system-name>, N_Port ID virtualization (NPIV) is not supported by fabric port connected to port <port>.`

Probable Cause N_Port ID virtualization (NPIV) capability is not supported by the fabric port to which the Access Gateway is connected.

Recommended Action

- On switches running Fabric OS 6.0 or earlier versions, run the **portCfgNpivPort** command to enable NPIV capability on the port connected to the Access Gateway. Refer to the *Fabric OS Command Reference* manual for more information on this command.
- Some blades and ports in a switch may not support NPIV. NPIV functionality can not be enabled on such ports and they will not respond to NPIV requests. Refer to the *Access Gateway Administrator Guide, Appendix B*, for specific AG-compatibility requirements.
- On non-Brocade switches, refer to the manufacturer's documentation to determine whether the switch supports NPIV and how to enable NPIV on these types of switches.

Severity ERROR

AG-1002

Message `<timestamp>, [AG-1002], <sequence-number>,, WARNING, <system-name>, Unable to find alternate N_Port during failover for N_Port <port>.`

Probable Cause Indicates no other N_Port is configured or the fabric was unstable during failover.

Recommended Action Check whether or not an alternate N_Port is configured.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AG-1003

Message `<timestamp>, [AG-1003], <sequence-number>,, WARNING, <system-name>, Unable to failover N_Port <port>. Failover across different fabrics is not supported.`

Probable Cause Indicates that the failover does not get blocked between two fabrics, although it is not a supported configuration.

Recommended Action Configure two or more N_Ports to connect to the same fabric; then execute the **ag --failoverenable** command to enable failover on these N_Ports.

Severity WARNING

AG-1004

Message `<timestamp>, [AG-1004], <sequence-number>,, ERROR, <system-name>, Invalid response to fabric login (FLOGI) request from the fabric for N_Port <port>.`

Probable Cause Indicates the fabric sent an invalid response to the FLOGI Extended Link Service (ELS) for the specified N_Port.

Recommended Action Check the configuration of the fabric switch.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AG-1005

Message `<timestamp>, [AG-1005], <sequence-number>,, WARNING, <system-name>, FDISC response was dropped because F_Port <port> is offline.`

Probable Cause Indicates the F_Port connected to the host is offline, which caused the FDISC response to drop.

Recommended Action Check the configuration of the host connected to the specified F_Port.

Severity WARNING

AG-1006

Message `<timestamp>, [AG-1006], <sequence-number>,, INFO, <system-name>, Access Gateway mode has been <msg>.`

Probable Cause Indicates Access Gateway mode has been enabled or disabled.

Recommended Action Run the **ag --modeshow** command to verify the current status of the Access Gateway mode.

Severity INFO

AG-1007

Message `<timestamp>, [AG-1007], <sequence-number>,, WARNING, <system-name>, FLOGI response not received for the N_Port <port> connected to the fabric.`

Probable Cause Indicates the N_Port connected to the fabric switch is not online. The specified N_Port has been disabled.

Recommended Action Check the connectivity between the Access Gateway N_Port and the fabric switch port.

Severity WARNING

AG-1008

Message `<timestamp>, [AG-1008], <sequence-number>,, WARNING, <system-name>, Invalid port login (PLOGI) response from the fabric on the N_Port <port>.`

Probable Cause Indicates the fabric switch management server did not accept the N_Port Login (PLOGI) request sent by the Access Gateway.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AG-1009

Message `<timestamp>, [AG-1009], <sequence-number>,, WARNING, <system-name>, Sending FLOGI failed on N_Port <port>.`

Probable Cause Indicates there was a failure sending a Fabric Login (FLOGI) request from the Access Gateway to the fabric switch.

Recommended Action Please check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AG-1010

Message `<timestamp>, [AG-1010], <sequence-number>,, WARNING, <system-name>, Sending PLOGI failed on N_Port <port>.`

Probable Cause Indicates there was a failure sending an N_Port Login (PLOGI) request from the Access Gateway to the fabric switch.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AG-1011

Message `<timestamp>, [AG-1011], <sequence-number>,, WARNING, <system-name>, Sending FDISC failed on N_Port <port>.`

Probable Cause Indicates there was a failure sending discover F_Port service parameter request from the Access Gateway to the fabric switch.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AG-1012

Message `<timestamp>, [AG-1012], <sequence-number>,, WARNING, <system-name>, Sending logout(LOGO)request failed on N_Port <port>.`

Probable Cause Indicates there was a failure sending an N_Port logout request from the Access Gateway to the fabric switch.

Recommended Action Check the configuration of the fabric switch connected to the Access Gateway.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AG-1013

Message `<timestamp>, [AG-1013], <sequence-number>,, INFO, <system-name>, F_Ports mapped to N_Port <port> failed over to other N_Ports.`

Probable Cause Indicates the specified N_Port is failing over to other N_Ports connected to the same fabric.

Recommended Action Run the **ag –mapShow** to display updated F_Port-to-N_Port mapping.

Severity INFO

AG-1014

Message `<timestamp>, [AG-1014], <sequence-number>,, INFO, <system-name>, Failing back F_Ports mapped to N_Port <port>.`

Probable Cause Indicates the specified N_Port is failing back F_Ports mapped to the specified N_Port.

Recommended Action Run the **ag –mapShow** command to display updated F_Port- to-N_Port mapping.

Severity INFO

AG-1015

Message `<timestamp>, [AG-1015], <sequence-number>,, WARNING, <system-name>, Unable to find online N_Ports to connect to the fabric.`

Probable Cause Indicates either no other N_Port is configured or all N_Ports are currently offline.

Recommended Action Check whether or not any other N_Port is configured.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportsave** command and contact your switch service provider.

Severity WARNING

AG-1016

Message `<timestamp>, [AG-1016], <sequence-number>,, INFO, <system-name>, Failing over F_Ports mapped to N_Port <port> to other N_Ports.`

Probable Cause Indicates the specified N_Port has failed to come online. All F_Ports mapped to this N_Port are being failed over to other active N_Ports.

Recommended Action Run the **ag –mapShow** command to display updated F_Port-to-N_Port mapping.

Severity INFO

AG-1017

Message `<timestamp>, [AG-1017], <sequence-number>,, WARNING, <system-name>, No N_Ports are currently Online.`

Probable Cause Indicates no N_Ports are currently configured in the system or all configured N_Ports have failed to come online.

Recommended Action Run the **switchShow** command to display the status of all ports in the system. Run the **portCfgShow** command to display a list of ports currently configured as N_Ports.

Severity WARNING

AG-1018

Message `<timestamp>, [AG-1018], <sequence-number>,, ERROR, <system-name>, Host port should not be connected to port <port>, which is configured as N_Port.`

Probable Cause Indicates that an Initiator or Target is erroneously connected to a port configured for N_Port operation.

Recommended Action Run the **switchShow** command to display the status of all ports in the system. Run the **portCfgShow** command to display a list of ports currently configured as N_Ports. Ensure that the host is connected to an F_port.

Severity ERROR

AG-1019

Message
```
<timestamp>, [AG-1019], <sequence-number>,, WARNING, <system-name>, Unable to
failover N_Port <port>. No other N Port in port group:<pgid> is online.
```

Probable Cause Indicates that failover across port groups is not supported.

Recommended Action Check whether or not an alternate N_Port is configured in this port group.

Severity WARNING

AG-1020

Message
```
<timestamp>, [AG-1020], <sequence-number>,, INFO, <system-name>, F_Ports to
N_Ports route/mapping has been changed.
```

Probable Cause Indicates that F_Port -to-N_Port mapping has been changed because the switch has come online or some new N_Port/F_Port has come online.

Recommended Action Run the **ag –mapshow** command to display the updated F_Port-to-N_Port mapping.

Severity INFO

AG-1021

Message
```
<timestamp>, [AG-1021], <sequence-number>,, WARNING, <system-name>, Unable to do
Preferred-Failover of F_Port <port>. Failover across different fabric is not
supported.
```

Probable Cause Indicates that the failover does not get blocked between two fabrics, although it is not a supported configuration.

Recommended Action Change the preferred N_Port settings for this F_Port using the **ag –prefset** command.

Choose the preferred N_Port such that it is in the same fabric as the primary N_Port of this F_Port. Use the **ag –show** command to check the fabric connectivity of N_Ports.

Severity WARNING

AG-1022

Message `<timestamp>, [AG-1022], <sequence-number>,, INFO, <system-name>, F_Port <fport> is failed over to its preferred N_Port <nport>.`

Probable Cause Indicates the specified F_Port is failing over to its preferred N_Port.

Recommended Action Run the **ag –mapshow** command to display the updated F_Port-to-N_Port mapping.

Severity INFO

AG-1023

Message `<timestamp>, [AG-1023], <sequence-number>,, INFO, <system-name>, F_Port <fport> mapped to offline N_Port <nport> is failed over to its preferred N_Port <pport>.`

Probable Cause Indicates the specified N_Port has failed to come online. The F_Port mapped to this N_Port had its preferred set and is online.

Recommended Action Run the **ag –mapshow** command to display updated F_Port -to -N_Port mapping.

Severity INFO

AG-1024

Message `<timestamp>, [AG-1024], <sequence-number>,, INFO, <system-name>, F_Port <fport> is failed back to its preferred N_Port <nport>.`

Probable Cause Indicates the specified N_Port is failing back F_Ports, which are failed over to some other N_Port.

Recommended Action Run the **ag –mapShow** command to display the updated F_Port-to-N_Port mapping.

Severity INFO

AG-1025

Message `<timestamp>, [AG-1025], <sequence-number>,, ERROR, <system-name>, Port group of Slave N_Port <port> is different than its Master N_Port <m_port>.`

Probable Cause Indicates that the port groups of the Master and Slave N_Ports are different while the Trunk Area assigned to the attached F_Ports on the edge switch is the same.

Recommended Action Run the **porttrunkarea –show** command on the attached switch to display that the Trunk Area is assigned to all ports in the system and run the **porttrunkarea –enable** command to reconfigure the Trunk Area.

Severity ERROR

AG-1026

Message `<timestamp>, [AG-1026], <sequence-number>,, WARNING, <system-name>, Unable to handle the login request on port <port> due to insufficient resources.`

Probable Cause Indicates there are insufficient resources.

Recommended Action Run configure CLI on AG switch and increase the number of allowed logins on this port.

If the message persists, run the **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AG-1027

Message `<timestamp>, [AG-1027], <sequence-number>,, WARNING, <system-name>, Unable to handle this login request on port <port> because NPIV capability is not enabled on this port.`

Probable Cause Indicates NPIV is not enabled.

Recommended Action Run the **portcfgnpivport** CLI command on the AG switch and enable the NPIV capability on this port.

Severity WARNING

AG-1028

Message `<timestamp>, [AG-1028], <sequence-number>,, WARNING, <system-name>, Device with Port WWN <port_name> tried to perform fabric login through port <fport>, without having access permission.`

Probable Cause Indicates the device does not have login access for that port, as per ADS policy set by the user.

Recommended Action Add the device in to the ADS allow list for that port using the **ag –adsadd** command.

Severity WARNING

AG-1029

Message `<timestamp>, [AG-1029], <sequence-number>,, WARNING, <system-name>, Port Group <pgid> has ports going to different fabrics.`

Probable Cause Indicates a misconfiguration.

Recommended Action Connect all ports in the port group to the same fabric.

Severity WARNING

AG-1030

Message `<timestamp>, [AG-1030], <sequence-number>,, WARNING, <system-name>, N_Port ID: <port> has been determined to be unreliable.`

Probable Cause Indicates that the port goes online and offline very often.

Recommended Action No action is required.

Severity WARNING

AG-1031

Message `<timestamp>, [AG-1031], <sequence-number>,, WARNING, <system-name>, Loop Detected for device with Port WWN <port> connected to port <port_name>`

Probable Cause Indicates that the routing Loop is detected for the device connected to the port.

Recommended Action Check the device configuration.

Severity WARNING

AG-1032

Message `<timestamp>, [AG-1032], <sequence-number>,, INFO, <system-name>, N-Port (ID: <port>) has recovered from an unreliable state.`

Probable Cause Indicates that the port state has been stable for the last five minutes.

Recommended Action No action is required.

Severity INFO

AG-1033

Message `<timestamp>, [AG-1033], <sequence-number>,, INFO, <system-name>,F_Port to N_Port mapping has been updated for N_Port (<n_port>) .`

Probable Cause Indicates that the F_Ports mapped to an N_Port have changed and the configuration file has been updated.

Recommended Action No action is required.

Severity INFO

AG-1034

Message `<timestamp>, [AG-1034], <sequence-number>,, INFO, <system-name>,F_Port cannot accept any more logins (<fport>) .`

Probable Cause Indicates that the F_Port has already logged in the maximum number of devices.

Recommended Action No action is required.

Severity INFO

AG-1035

Message `<timestamp>, [AG-1035], <sequence-number>,, INFO, <system-name>,Device cannot login as ALPA value not available (<alpa>) .`

Probable Cause Indicates that a device has already used this ALPA value.

Recommended Action No action is required.

Severity INFO

AG-1036

Message `<timestamp>, [AG-1036], <sequence-number>,, WARNING, <system-name>,Port <port> is connected to a Non-Brocade fabric with Persistent ALPA enabled. Check the admin guide for supported configuration .`

Probable Cause Indicates that one of the ports is connected to a non-Brocade fabric.

Recommended Action No action is required.

Severity WARNING

AG-1037

Message `<timestamp>, [AG-1037], <sequence-number>,, INFO, <system-name>,Trunked N_Port (<nport>) going offline, if switchshow CLI for the connected fabric switch port displays Persistently disabled: Area has been acquired, then check cabling: all trunked ports should be in same ASIC Port Group .`

Probable Cause Indicates that the cabling is incorrect.

Recommended Action If the **switchshow** command on the connected fabric switch port displays 'Persistently disabled: Area has been acquired', then check the cabling on the AG. All trunked ports in a single trunk should belong to the same ASIC Port Group.

Severity INFO

AG-1038

Message `<timestamp>, [AG-1038], <sequence-number>,, ERROR, <system-name>,Elara Ports going to different fabrics, Check N Port <nport>.`

Probable Cause Indicates a misconfiguration.

Recommended Action Connect all ports in the port group to the same fabric.

Severity ERROR

AG-1039

Message `<timestamp>, [AG-1039], <sequence-number>,, INFO, <system-name>,F-Port <Port that was reset> was reset because a WWN mapped device using it, through N-Port <Port who's state change caused the reset>, went offline.`

Probable Cause Indicates a port needed to be reset because an N-Port went offline and the changes need to be propagated to all involved devices.

Recommended Action No action is required. This port-reset was not an error.

Severity INFO

Chapter

AN System Messages

3

AN-1001

Message `<timestamp>, [AN-1001], <sequence-number>,, ERROR, <system-name>, Failed to allocate memory: <function name>`

Probable Cause Indicates that the specified function has failed to allocate memory.

Recommended Action Check memory usage on the switch using the **memShow** command. Restart or power cycle the switch.

Severity ERROR

AN-1002

Message `<timestamp>, [AN-1002], <sequence-number>,, ERROR, <system-name>, Failed to initialize; rc = <error>`

Probable Cause Indicates that the initialization of the 'trafd' daemon has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

AN-1003

Message `<timestamp>, [AN-1003], <sequence-number>,, WARNING, <system-name>, Latency bottleneck at slot <slot number>, port <port number within slot number>. <percentage of seconds affected by latency bottlenecking>.2f percent of last <observation period over which the percentage of affected seconds is reported> seconds were affected. Avg. inter-frame time <observed frame rate>.4f us.`

Probable Cause For an F_Port, it indicates that the attached device is slow in responding to frames going out of this port. This latency may be inherent in the device or due to heavy workload on the device. For an E_Port, it indicates a downstream primary bottleneck.

Recommended Action Find the Top Talkers in the egress direction from this port and apply Ingress Rate Limiting to one or more of them.

Severity WARNING

AN-1004

Message `<timestamp>, [AN-1004], <sequence-number>,, WARNING, <system-name>, Slot <slot number>, port <port number within slot number> is a congestion bottleneck. <percentage of seconds affected by congestion bottlenecking> percent of last <observation period over which the percentage of affected seconds is reported> seconds were affected by this condition.`

Probable Cause Indicates that the volume of outgoing traffic at this port is too high for the capacity of the link.

Recommended Action Add more capacity on the path, using trunk links if possible.

Severity WARNING

AN-1005

Message `<timestamp>, [AN-1005], <sequence-number>,, WARNING, <system-name>, Slot <slot number>, port <port number within slot number> has <bottleneck type> bottleneck cleared.`

Probable Cause Indicates that the bottleneck was cleared on the port.

Recommended Action No action is required.

Severity WARNING

AN-1010

Message `<timestamp>, [AN-1010], <sequence-number>,, WARNING, <system-name>, Severe latency bottleneck detected at Slot <slot number> port <port number within slot number>.`

Probable Cause Indicates a credit loss.

Recommended Action Contact your vendor's customer support for assistance.

Severity WARNING

Chapter

4

AUTH System Messages

AUTH-1001

Message `<timestamp>, [AUTH-1001], <sequence-number>,, INFO, <system-name>, <Operation type> has been successfully completed.`

Probable Cause Indicates that the secret database operation has been updated using the **secAuthSecret** command. The values for *Operation type* can be “set” or “remove”.

Recommended Action No action is required.

Severity INFO

AUTH-1002

Message `<timestamp>, [AUTH-1002], <sequence-number>,, ERROR, <system-name>, <Operation type> has failed.`

Probable Cause Indicates that the specified action has failed to update the secret database using the **secAuthSecret** command. The values for *Operation type* can be “set” or “remove”.

Recommended Action Retry the **secAuthSecret** command.

Run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1003

Message `<timestamp>, [AUTH-1003], <sequence-number>,, INFO, <system-name>, <data type> type has been successfully set to <setting value>.`

Probable Cause Indicates that an authentication configuration value was set to the specified value. The *data type* is either authentication type, DH group type, or policy type.

Recommended Action No action is required.

Severity INFO

AUTH-1004

Message `<timestamp>, [AUTH-1004], <sequence-number>,, ERROR, <system-name>, Failed to set <data type> type to <setting value>.`

Probable Cause Indicates that the **authUtil** command has failed to set the authentication configuration value. The *data type* is either authentication type, DH group type, or policy type.

Recommended Action Retry the **authUtil** command.

Run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1005

Message `<timestamp>, [AUTH-1005], <sequence-number>,, ERROR, <system-name>, Authentication file does not exist: <error code>.`

Probable Cause Indicates an authentication file corruption.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

Run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1006

Message `<timestamp>, [AUTH-1006], <sequence-number>,, WARNING, <system-name>, Failed to open authentication configuration file.`

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AUTH-1007

Message `<timestamp>, [AUTH-1007], <sequence-number>,, ERROR, <system-name>, The proposed authentication protocols are not supported: port <port number>.`

Probable Cause Indicates that the proposed authentication protocol type or types are not supported by the local specified port.

Recommended Action Run the **authUtil** command to make sure the local switch supports the specified protocols: Fibre channel authentication protocol (FCAP) or Diffie Hellman - challenge handshake authentication protocol (DH-CHAP).

Severity ERROR

AUTH-1008

Message `<timestamp>, [AUTH-1008], <sequence-number>,, ERROR, <system-name>, No security license, operation failed.`

Probable Cause Indicates that the switch does not have a security license.

Recommended Action Verify that the security license is installed using the **licenseShow** command. If necessary, reinstall the license using the **licenseAdd** command.

Severity ERROR

AUTH-1010

Message `<timestamp>, [AUTH-1010], <sequence-number>,, ERROR, <system-name>, Failed to initialize security policy: switch <switch number>, error <error code>.`

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reboot or power cycle the switch.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1011

Message `<timestamp>, [AUTH-1011], <sequence-number>,, WARNING, <system-name>, Failed to register for failover operation: switch <switch number> error <error code>.`

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AUTH-1012

Message `<timestamp>, [AUTH-1012], <sequence-number>,, WARNING, <system-name>, Authentication <code> is rejected: port <port number> explain <explain code> reason <reason code>.`

Probable Cause Indicates that an authentication is rejected because the remote entity does not support authentication.

Recommended Action Make sure the entity at the other end of the link supports authentication.

Severity WARNING

AUTH-1013

Message `<timestamp>, [AUTH-1013], <sequence-number>,, WARNING, <system-name>, Can not perform authentication request message: port <port number>, message code <message code>.`

Probable Cause Indicates that the system is running low on resources when receiving an authentication request.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

AUTH-1014

Message `<timestamp>, [AUTH-1014], <sequence-number>, FFDC, ERROR, <system-name>, Invalid port value to <operation>: port <port number>.`

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1016

Message `<timestamp>, [AUTH-1016], <sequence-number>, FFDC, ERROR, <system-name>, Invalid value to start HBA authentication port: <port number>, <pid>.`

Probable Cause This may relate to an internal failure.

Recommended Action Copy the message, collect switch information using the **supportShow** command, and contact your switch service provider.

Severity ERROR

AUTH-1017

Message `<timestamp>, [AUTH-1017], <sequence-number>,, ERROR, <system-name>, Invalid value to start authentication request: port <port number>, operation code <operation code>.`

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1018

Message `<timestamp>, [AUTH-1018], <sequence-number>,, ERROR, <system-name>, Invalid value to check protocol type: port <port number>.`

Probable Cause Indicates an internal problem with the Secure Fabric OS.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1020

Message `<timestamp>, [AUTH-1020], <sequence-number>,, INFO, <system-name>, Failed to create timer for authentication: port <port number>.`

Probable Cause Indicates that an authentication message's timer was not created.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

AUTH-1022

Message `<timestamp>, [AUTH-1022], <sequence-number>,, ERROR, <system-name>, Failed to extract <data type> from <message> payload: port <port number>.`

Probable Cause Indicates that the authentication process failed to extract a particular value from the receiving payload.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1023

Message `<timestamp>, [AUTH-1023], <sequence-number>,, ERROR, <system-name>, Failed to <operation type> during <authentication phase>: port <port number>.`

Probable Cause Indicates an authentication operation failed for a certain authentication phase.

Operation type varies depending on authentication type:

- Some operations for switch link authentication protocol (SLAP): certificate retrieve, certificate verification, signature verification, or nonce signing.
- Some operations for fibre channel authentication protocol (FCAP): certificate retrieve, certificate verification, signature verification, or nonce singing.
- Some operations for Diffie Hellman - challenge handshake authentication Protocol (DH-CHAP). response calculation, challenge generation, or secret retrieve.

The *authentication phase* specifies which phase of a particular authentication protocol failed.

A *nonce* is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Recommended Action The error might indicate that an invalid entity tried to connect to the switch. Check the connection port for possible unauthorized access attack.

It might indicate that the public key infrastructure (PKI) object for SLAP or FCAP or secret value for DH-CHAP on the local entity is not set up properly. Reinstall all PKI objects or reset the secret value for DH-CHAP properly.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1025

Message `<timestamp>, [AUTH-1025], <sequence-number>,, ERROR, <system-name>, Failed to get <data type> during <authentication phase>: port <port number>.`

Probable Cause Indicates that the authentication process failed to get the expected information during the specified authentication phase.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1026

Message `<timestamp>, [AUTH-1026], <sequence-number>,, WARNING, <system-name>, Failed to get <Device information> during negotiation phase: port <port number>.`

Probable Cause Indicates that the authentication failed to get device or host bus adaptor (HBA) information due to an internal failure.

Recommended Action Usually this problem is transient. If the authentication failed, retry the login.

Reinitialize authentication using the **switchDisable** and **switchEnable** commands or the **portDisable** and **portEnable** commands.

Severity WARNING

AUTH-1027

Message `<timestamp>, [AUTH-1027], <sequence-number>,, ERROR, <system-name>, Failed to select <authentication value> during <authentication phase>: value <value> port <port number>.`

Probable Cause Indicates that the authentication process failed to select an *authentication value* (that is, DH Group, hash value, or protocol type) from a receiving payload for the specified *authentication phase*. This indicates that the local switch does not support the specified authentication value.

Recommended Action Check the authentication configuration and reset the supported value if needed using the **authUtil** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1028

Message `<timestamp>, [AUTH-1028], <sequence-number>,, ERROR, <system-name>, Failed to allocate <data type> for <operation phase>: port <port number>.`

Probable Cause Indicates that the authentication process failed because the system is low on memory.

Data type is the payload or structure that failed to get memory. *Operation phase* specifies which operation of a particular authentication phase failed.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1029

Message `<timestamp>, [AUTH-1029], <sequence-number>,, ERROR, <system-name>, Failed to get <data type> for <message phase> message: port <port number>, retval <error code>.`

Probable Cause Indicates that the authentication process failed to get a particular authentication value at certain phase.

Data type is the payload or structure that failed to get memory.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1030

Message `<timestamp>, [AUTH-1030], <sequence-number>,, ERROR, <system-name>, Invalid message code for <message phase> message: port <port number>.`

Probable Cause Indicates the receiving payload does not have valid message code for a particular authentication phase.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1031

Message `<timestamp>, [AUTH-1031], <sequence-number>,, ERROR, <system-name>, Failed to retrieve secret value: port <port number>.`

Probable Cause Indicates that the secret value was not set properly for the authenticated entity.

Recommended Action Reset the secret value by using the **secAuthSecret** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

Severity ERROR

AUTH-1032

Message `<timestamp>, [AUTH-1032], <sequence-number>,, ERROR, <system-name>, Failed to generate <data type> for <message payload> payload: length <data length>, error code <error code>, port <port number>.`

Probable Cause Indicates that the authentication process failed to generate specific data (that is, challenge, nonce, or response data) for an authentication payload. This usually relates to internal failure.

A nonce is a single-use, usually random value used in authentication protocols to prevent replay attacks.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1033

Message `<timestamp>, [AUTH-1033], <sequence-number>,, ERROR, <system-name>, Disable port <port number> due to unauthorized switch <switch WWN value>.`

Probable Cause Indicates that an entity was not configured in the switch connection control (SCC) policy and tried to connect to the port.

Recommended Action Add the entity's world wide name (WWN) to the SCC policy and reinitialize authentication by using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

Severity ERROR

AUTH-1034

Message `<timestamp>, [AUTH-1034], <sequence-number>,, ERROR, <system-name>, Failed to validate name <entity name> in <authentication message>: port <port number>.`

Probable Cause Indicates that the specified entity name in the payload is not in the correct format.

Recommended Action Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1035

Message `<timestamp>, [AUTH-1035], <sequence-number>,, ERROR, <system-name>, Invalid <data type> length in <message phase> message: length <data length>, port <port number>.`

Probable Cause Indicates that a particular data field in the authentication message has an invalid length field. This error usually relates to internal failure.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1036

Message `<timestamp>, [AUTH-1036], <sequence-number>,, ERROR, <system-name>, Invalid state <state value> for <authentication phase>: port <port number>.`

Probable Cause Indicates that the switch received an unexpected authentication message.

Recommended Action Usually this problem is transient. The authentication might fail.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1037

Message `<timestamp>, [AUTH-1037], <sequence-number>,, ERROR, <system-name>, Failed to <operation type> response for <authentication message>: init_len <data length>, resp_len <data length>, port <port number>.`

Probable Cause Indicates that a Diffie Hellman - challenge handshake authentication protocol (DH-CHAP) authentication operation failed on the specified port due to mismatched response values between two entities.

Recommended Action The error might indicate that an invalid entity tried to connect to the switch. Check the connection port for a possible security attack.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1038

Message `<timestamp>, [AUTH-1038], <sequence-number>,, ERROR, <system-name>, Failed to retrieve certificate during <authentication phase>: port <port number>.`

Probable Cause Indicates that the public key infrastructure (PKI) certificate is not installed properly.

Recommended Action Reinstall the PKI certificate, using the **pkiCreate** command.

Reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1039

Message `<timestamp>, [AUTH-1039], <sequence-number>,, ERROR, <system-name>, Neighboring switch has conflicting authentication policy: Port <Port Number> disabled.`

Probable Cause Indicates that the neighboring switch has a conflicting authentication policy enabled. The_E-Port has been disabled, because the neighboring switch rejected the authentication negotiation, and the local switch has a strict switch authentication policy.

Recommended Action Correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the port using the **portEnable** command.

Severity ERROR

AUTH-1040

Message `<timestamp>, [AUTH-1040], <sequence-number>,, INFO, <system-name>, Reject authentication on port <Port Number>, because switch authentication policy is set to OFF.`

Probable Cause Indicates that the local switch has rejected the authentication because the switch policy is turned off. If the neighboring switch has a strict (ON) switch policy, the light will go off due to conflicting configuration settings. Otherwise E_Port will form without authentication.

Recommended Action If there is no light on the port, correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the port on the neighboring switch using the **portEnable** command. If the E_Port formed, no action is required.

Severity INFO

AUTH-1041

Message `<timestamp>, [AUTH-1041], <sequence-number>,, ERROR, <system-name>, Port <port number> has been disabled, because an authentication-reject was received with code '<Reason String>' and explanation '<Explanation String>'.`

Probable Cause The specified port had been disabled, because it received an authentication-reject response from the connected switch/device. The error might indicate that an invalid entity attempted to connect to the switch.

Recommended Action Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1042

Message `<timestamp>, [AUTH-1042], <sequence-number>,, ERROR, <system-name>, Port <port number> has been disabled, because authentication failed with code '<Reason String>' and explanation '<Explanation String>'.`

Probable Cause The specified port has been disabled, because the connecting switch/device failed to authenticate. The error might indicate that an invalid entity attempted to connect to the switch.

Recommended Action Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1043

Message `<timestamp>, [AUTH-1043], <sequence-number>,, ERROR, <system-name>, Failed to enforce device authentication mode:<Device Auth Policy>(error: <Reason Code>).`

Probable Cause Indicates that the Kernel mode setting for F_Port authentication failed. Device authentication will be defaulted to OFF, and switch will not participate in Diffie Hellman - challenge handshake authentication protocol (DH-CHAP) authentication with devices.

Recommended Action Try setting the device authentication policy manually using the **authUtil** command.

Severity ERROR

AUTH-1044

Message `<timestamp>, [AUTH-1044], <sequence-number>,, ERROR, <system-name>, Authentication <Reason for disabling the port>. Disabling port <port number>.`

Probable Cause Indicates authentication has timed out after multiple retries. The specified port has been disabled as a result. This problem may be transient due to the system's central processing unit (CPU) load. In addition, a defective small form-factor pluggable (SFP) or faulty cable may have caused the failure.

Recommended Action Check the SFP and the cable. Then try to enable the port using the **portEnable** command.

Severity ERROR

AUTH-1045

Message `<timestamp>, [AUTH-1045], <sequence-number>,, ERROR, <system-name>, Certificate not present in this switch in <authentication phase> port <port number>.`

Probable Cause Indicates that the public key infrastructure (PKI) certificate is not installed in this switch.

Recommended Action Check the certificate availability using the **pkiShow** command. Install the certificate and reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1046

Message `<timestamp>, [AUTH-1046], <sequence-number>,, INFO, <system-name>, <Operation type> has been successfully completed.`

Probable Cause Indicates that the certificate database operation has been updated using the **secAuthCertificate** command. The values for Operation type can be "set" or "remove".

Recommended Action No action is required.

Severity INFO

AUTH-1047

Message `<timestamp>, [AUTH-1047], <sequence-number>,, ERROR, <system-name>, <Operation type> has failed.`

Probable Cause Indicates that the specified action has failed to update the certificate database using the **secAuthCertificate** command. The values for Operation type can be "set" or "remove".

Recommended Action Retry the **secAuthCertificate** command.

Run supportFtp (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

Chapter

ANV System Messages

5

ANV-1001

Message `<timestamp>, [ANV-1001], <sequence-number>,, ERROR, <system-name>, Port <port number> port fault. Please change the SFP or check cable.`

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP), an incompatible SFP pair, or a faulty cable between peer ports.

Recommended Action Verify if you are using compatible SFPs on the peer ports. Verify if the SFPs have deteriorated and if the Fibre Channel cable is faulty. Replace the SFPs or the cable if necessary.

Severity ERROR

ANV-1002

Message `<timestamp>, [ANV-1002], <sequence-number>,Ffdc, ERROR, <system-name>, Port <port number> chip faulted due to internal error.`

Probable Cause Indicates an internal error. All the ports on the blade or switch will be disrupted.

Recommended Action For a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade to recover the system. For a non-bladed system, perform the **fastBoot** command on the switch to recover the system.

Severity ERROR

ANV-1003

Message `<timestamp>, [ANV-1003], <sequence-number>,, CRITICAL, <system-name>, <slot number>,<chip index>: HW ASIC Chip error. Type = 0x<chip error type>, Error = <chip error string>..`

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade data traffic.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the blade.

Severity CRITICAL

ANV-1004

Message `<timestamp>, [ANV-1004], <sequence-number>,, ERROR, <system-name>, <slot number>,<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address> bad_addr:0x<Bad address>.`

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that may degrade data traffic.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the blade.

Severity ERROR

ANV-1005

Message `<timestamp>, [ANV-1005], <sequence-number>,, ERROR, <system-name>,<slot number>,<chip index>,<anvil id>: Memory allocation failed.`

Probable Cause Indicates the memory allocation failure in the software.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the CP blade.

Severity ERROR

ANV-1006

Message `<timestamp>, [ANV-1006], <sequence-number>,, CRITICAL, <system-name>, <slot number>,<chip index>: HW ASIC Chip fault. Type = 0x<chip error type>, Error = <chip error string>.`

Probable Cause Indicates an internal error in the application-specific integrated circuit (ASIC) hardware that renders the chip as not operational.

Recommended Action Restart the system at the next maintenance window. If the problem persists, replace the blade.

Severity CRITICAL

ANV-1007

Message `<timestamp>, [ANV-1007], <sequence-number>,, CRITICAL, <system-name>, <slot number>,<chip index>: ANVIL PASS 1 low buff pool fault: <chip regval field> 0x<chip error type>.`

Probable Cause Indicates that Anvil Pass 1 is out of free buffer which might cause a chip fault.

Recommended Action Reconfigure the testing setup.

Severity CRITICAL

Chapter

BKSW System Messages

6

BKSW-1003

Message `<timestamp>, [BKSW-1003], <sequence-number>,, WARNING, <system-name>, kSWD: <warning message>.`

Probable Cause Indicates a warning state within the system.

A critical application error was reported in the watchdog subsystem. This message is used to convey information regarding the state of the system. Refer to the string at the end of the error message for specific information. The switch will reboot (on single-CP switches) or fail over (on dual-CP switches).

The warning message will be one of the following:

- <Detected unexpected termination of: <daemon name>>
  Probable Cause: One of the critical daemons ended unexpectedly.
- <<daemon name> failed to refresh SWD*** Sending SIGABRT to PID <process id number>>
  Probable Cause: One of the critical daemons is found to be nonresponsive; sending signal abort.

Recommended Action Run the **supportSave** command to determine if any core files were created. If a core file is found, run **supportFtp** to send all the core files to a secure server location.

Copy the error message and any core file information, and contact your switch service provider.

Severity WARNING

Chapter

BL System Messages

7

BL-1000

Message `<timestamp>, [BL-1000], <sequence-number>,, INFO, <system-name>, Initializing ports...`

Probable Cause Indicates that the switch has started initializing the ports.

Recommended Action No action is required.

Severity INFO

BL-1001

Message `<timestamp>, [BL-1001], <sequence-number>,, INFO, <system-name>, Port initialization completed.`

Probable Cause Indicates that the switch has completed initializing the ports.

Recommended Action No action is required.

Severity INFO

BL-1002

Message `<timestamp>, [BL-1002], <sequence-number>, FFDC, CRITICAL, <system-name>, Init Failed: slot <slot number> DISABLED because internal ports were not ONLINE, <list of internal port number not ONLINE>.`

Probable Cause Indicates that the blade initiation failed because one or more of the internal ports were not online. The blade is faulted.

Recommended Action Make sure that the blade is seated correctly. If the blade is seated correctly, restart or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. To run this command root access is required. To run this command root access is required. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Additional blade fault messages precede and follow this error, providing more information. See other error messages for recommended action.

If the message persists, replace the blade.

Severity CRITICAL

BL-1003

Message `<timestamp>, [BL-1003], <sequence-number>, FFDC, CRITICAL, <system-name>, Faulting blade in slot <slot number>.`

Probable Cause Indicates a faulty blade in the specified slot number.

Recommended Action Make sure that the blade is seated correctly. If the blade is seated correctly, restart or power cycle the blade.

Run the **systemVerification** command to verify that blade does not have hardware problems. To run this command root access is required. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *Fabric OS Command Reference* for more information on these commands.

If the message persists, replace the blade.

Severity CRITICAL

BL-1004

Message `<timestamp>, [BL-1004], <sequence-number>, FFDC, CRITICAL, <system-name>, Suppressing blade fault in slot <slot number>.`

Probable Cause Indicates that the specified blade experienced a failure but was not faulted due to a user setting.

Recommended Action Restart or power cycle the blade, using the **slotPowerOff** and **slotPowerOn** commands.

Run the **systemVerification** command to verify that the blade does not have hardware problems. To run this command root access is required. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *Fabric OS Command Reference* for more information on these commands.

If the message persists, replace the blade.

Severity CRITICAL

BL-1006

Message `<timestamp>, [BL-1006], <sequence-number>,, INFO, <system-name>, Blade <slot number> NOT faulted. Peer blade <slot number> experienced abrupt failure.`

Probable Cause Indicates that the errors (mostly synchronization errors) on this blade are harmless. Probably, the standby control processor (CP) blade connected to the active CP blade has experienced transitory problems.

Recommended Action Use the **haShow** command to verify that the standby CP is healthy. If problem persists remove and reinstall the faulty blade.

Severity INFO

BL-1007

Message `<timestamp>, [BL-1007], <sequence-number>,, WARNING, <system-name>, blade #<blade number>: blade state is inconsistent with EM. bl_cflags 0x<blade control flags>, slot_on <slot_on flag>, slot_off <slot_off flag>, faulty <faulty flag>, status <blade status>.`

Probable Cause Indicates that a failover occurred while a blade was initializing on the previously active control processor (CP).

Recommended Action No action is required. The blade is reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity WARNING

BL-1008

Message `<timestamp>, [BL-1008], <sequence-number>, FFDC, CRITICAL, <system-name>, Slot <slot number> control-plane failure. Expected value: 0x<value 1>, Actual: 0x<value 2>.`

Probable Cause Indicates that the blade has experienced a hardware failure or was removed without following the recommended removal procedure.

Recommended Action Make sure that the blade is seated correctly.

If the blade is seated correctly, restart or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. To run this command root access is required. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *Fabric OS Command Reference* for more information on these commands.

If the message persists, replace the blade.

Severity CRITICAL

BL-1009

Message `<timestamp>, [BL-1009], <sequence-number>, FFDC, CRITICAL, <system-name>, Blade in slot <slot number> timed out initializing the chips.`

Probable Cause Indicates that the blade has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended Action Make sure that the blade is seated correctly.

If the blade is seated correctly, reboot or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. To run this command root access is required. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *Fabric OS Command Reference* for more information on these commands.

If the message persists, replace the blade.

Severity CRITICAL

BL-1010

Message `<timestamp>, [BL-1010], <sequence-number>,, WARNING, <system-name>, Blade in slot <slot number> inconsistent with the hardware settings.`

Probable Cause Indicates that a failover occurred while some hardware changes were being made on the previously active control processor (CP) (such as changing the domain ID).

Recommended Action No action is required. This blade has been reinitialized. Because reinitializing a blade is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity WARNING

BL-1011

Message `<timestamp>, [BL-1011], <sequence-number>, FFDC, CRITICAL, <system-name>, Busy with emb-port int. for chip <chip number> in minis <minis number> on blade <slot number>, chip int. is disabled. interrupt status=0x<interrupt status>.`

Probable Cause Indicates that too many interrupts in the embedded port caused the specified chip to be disabled. The probable cause is too many abnormal frames; the chip is disabled to prevent the control processor (CP) from becoming too busy.

Recommended Action Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP), or device attached to the specified port.

Run the **systemVerification** command to verify that the blade or switch does not have hardware problems. To run this command root access is required.

Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, restart or power cycle the switch.

If the message persists, replace the blade or the (nonbladed) switch.

Severity CRITICAL

BL-1012

Message `<timestamp>, [BL-1012], <sequence-number>,, ERROR, <system-name>, bport <port number> port int. is disabled. status=0x<interrupt status> Port <port number> will be re-enabled in 1 minute.`

Probable Cause Indicates that the port generated an excessive number of interrupts that might prove unrecoverable to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* is the blade port; this number might not correspond to a user port number.

Recommended Action Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP), or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, restart or power cycle the switch.

If the message persists, replace the blade or the (nonbladed) switch.

Severity ERROR

BL-1013

Message

```
<timestamp>, [BL-1013], <sequence-number>,, ERROR, <system-name>, bport <port
number> port is faulted. status=0x<interrupt status> Port <port number> will be
re-enabled in 1 minute.
```

Probable Cause Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* is the blade port; this number might not correspond to a user port number.

Recommended Action Make sure to capture the console output during this process.

Check for a faulty cable, small form-factor pluggable (SFP), or device attached to the specified port.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, restart or power cycle the switch.

If the message persists, replace the blade.

Severity ERROR

BL-1014

Message

```
<timestamp>, [BL-1014], <sequence-number>,, ERROR, <system-name>, bport <port
number> port int. is disabled. status=0x<interrupt status>.
```

Probable Cause Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the control processor (CP) from becoming too busy. The *bport* is the blade port; this number might not correspond to a user port number.

Recommended Action Make sure to capture the console output during this process.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, **reboot** the switch.

Run the **systemVerification** command to determine if there is a hardware error. To run this command root access is required.

Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled.

If there is a hardware error, if the **slotPowerOff** or **slotPowerOn** fails on the bladed switch or if errors are encountered again:

- On the Brocade 24000, and 48000, replace the blade field-replaceable unit (FRU).
- On the Brocade 3900, replace the motherboard FRU.
- On the Brocade 200E, 3016, 3250, 3850, or 4100, 4012, 4016, 4018, 4024, 4900, 7500, AP7600, and 5000, replace the switch.

Severity ERROR

BL-1015

Message `<timestamp>, [BL-1015], <sequence-number>,, ERROR, <system-name>, bport <port number> port is faulted. status=0x<interrupt status>.`

Probable Cause Indicates that the port generated an excessive number of interrupts that might prove fatal to the switch operation. The port is disabled to prevent the CP from becoming too busy. The *bport* is the blade port; this number might not correspond to a user port number.

Recommended Action Make sure to capture the console output during this process.

On a bladed switch, run the **slotPowerOff** and **slotPowerOn** commands.

On a nonbladed switch, **reboot** the switch.

Run the **systemVerification** command to determine if there is a hardware error. To run this command root access is required.

Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled.

If there is a hardware error, if the **slotPowerOff** or **slotPowerOn** fails on the bladed switch or if errors are encountered again:

- On the Brocade 24000, and 48000, replace the blade field-replaceable unit (FRU).
- On the Brocade 3900, replace the motherboard FRU.
- On the Brocade 200E, 3016, 3250, 3850, or 4100, 4012, 4016, 4018, 4024, 4900, 7500, AP7600, and 5000, replace the switch.

Severity ERROR

BL-1016

Message `<timestamp>, [BL-1016], <sequence-number>, FFDC, CRITICAL, <system-name>, Blade port <port number> in slot <slot number> failed to enable.`

Probable Cause Indicates that the specified blade port has failed to get enabled.

Recommended Action Make sure that the blade is seated correctly.

If the blade is seated correctly, restart or power cycle the blade.

Run the **systemVerification** command to verify that the blade does not have hardware problems. To run this command root access is required. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *Fabric OS Command Reference* for more information on these commands.

If the message persists, replace the blade.

Severity CRITICAL

BL-1017

Message `<timestamp>, [BL-1017], <sequence-number>,, INFO, <system-name>, Slot <slot number> Initializing...`

Probable Cause Indicates that the slot has started initializing the ports.

Recommended Action No action is required.

Severity INFO

BL-1018

Message `<timestamp>, [BL-1018], <sequence-number>,, INFO, <system-name>, Slot <slot number> Initialization completed.`

Probable Cause Indicates that the slot has completed initializing the ports.

Recommended Action No action is required.

Severity INFO

BL-1019

Message `<timestamp>, [BL-1019], <sequence-number>,, INFO, <system-name>, Slot <Slot number>, retry <Retry Number>, internal port retry initialization, <List of internal ports retrying initialization>.`

Probable Cause Indicates that the slot had internal ports not online and that the system is retrying to bring the ports that failed back online.

Recommended Action No action is required.

Severity INFO

BL-1020

Message `<timestamp>, [BL-1020], <sequence-number>,, CRITICAL, <system-name>, Switch timed out initializing the chips.`

Probable Cause Indicates that the switch has failed to initialize the application-specific integrated circuit (ASIC) chips.

Recommended Action Restart or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. To run this command root access is required. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *Fabric OS Command Reference* for more information on these commands.

If the message persists, replace the switch.

Severity CRITICAL

BL-1021

Message `<timestamp>, [BL-1021], <sequence-number>,, INFO, <system-name>, Retry <Retry Number>, internal port retry initialization, <List of internal ports retrying initialization>.`

Probable Cause Indicates that the switch had internal ports not online and that the system is retrying to bring the ports that failed back online.

Recommended Action No action is required.

Severity INFO

BL-1022

Message `<timestamp>, [BL-1022], <sequence-number>,, CRITICAL, <system-name>, Init Failed: Switch DISABLED because internal ports were not ONLINE, <list of internal port number not ONLINE>.`

Probable Cause Indicates that the switch initiation failed because one or more of the internal ports was not online. The switch is faulted.

Recommended Action Restart or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. To run this command root access is required. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. Refer to the *Fabric OS Command Reference* for more information on these commands.

Additional fault messages precede and follow this error, providing more information. See other error messages for recommended action.

If the message persists, replace the switch.

Severity CRITICAL

BL-1023

Message `<timestamp>, [BL-1023], <sequence-number>,, CRITICAL, <system-name>, Blade in slot <slot number> was reset before blade init completed. As a result the blade is faulted.`

Probable Cause Indicates that the blade was reset before the initialization completed.

Recommended Action Restart or power cycle the blade.

If the message persists, replace the blade.

Severity CRITICAL

BL-1024

Message `<timestamp>, [BL-1024], <sequence-number>,, INFO, <system-name>, All ports on the blade in slot <slot number> will be reset as part of the firmware upgrade.`

Probable Cause Indicates that a recent firmware upgrade caused the blade's firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all datapath elements were reset.

Recommended Action No action is required.

Severity INFO

BL-1025

Message `<timestamp>, [BL-1025], <sequence-number>,, INFO, <system-name>, All GigE/FCIP Virtualization ports on the blade in slot <slot number> will be reset as part of the firmware upgrade.`

Probable Cause Indicates that a recent firmware upgrade caused the blade's firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all GbE or Fibre Channel over IP (FCIP) or Virtualization data elements or FC Fastwrite ports were reset.

Recommended Action No action is required.

Severity INFO

BL-1026

Message `<timestamp>, [BL-1026], <sequence-number>,, CRITICAL, <system-name>, Internal port offline during warm recovery, state <port state> (0x<port ID>).`

Probable Cause Indicates that an internal port went offline during the warm recovery of the switch. The switch will reboot and start a cold recovery.

Recommended Action Collect **supportSave** information, then restart the switch and run the **diagPost** command to ensure Power-On Self-Test (POST) is enabled. If the problem persists, replace the switch.

Severity CRITICAL

BL-1027

Message `<timestamp>, [BL-1027], <sequence-number>,, CRITICAL, <system-name>, Blade in slot <slot number> faulted, boot failed; status 0x<boot status> 0x<1250 0 boot status> 0x<1250 1 boot status>.`

Probable Cause Indicates that the blade failed to boot properly.

Recommended Action Restart or power cycle the blade.

If the message persists, replace the blade.

Severity CRITICAL

BL-1028

Message `<timestamp>, [BL-1028], <sequence-number>,, CRITICAL, <system-name>, Switch faulted; internal processor was reset before switch init completed.`

Probable Cause Indicates that the switch's internal processor was reset before the initialization completed.

Recommended Action Restart or power cycle the switch.

If the message persists, replace the switch.

Severity CRITICAL

BL-1029

Message `<timestamp>, [BL-1029], <sequence-number>,, INFO, <system-name>, All ports on the switch will be reset as part of the firmware upgrade.`

Probable Cause Indicates that a recent firmware upgrade caused the switch's internal processor firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all the datapath elements were reset.

Recommended Action No action is required.

Severity INFO

BL-1030

Message `<timestamp>, [BL-1030], <sequence-number>,, INFO, <system-name>, All GigE/FCIP Virtualization/FC Fastwrite ports on the switch will be reset as part of the firmware upgrade.`

Probable Cause Indicates that a recent firmware upgrade caused the switch's internal processor firmware to be upgraded and resulted in the cold upgrade. As part of the upgrade, all the GbE or Fibre Channel over IP (FCIP) or Virtualization data elements or FC Fastwrite ports were reset.

Recommended Action No action is required.

Severity INFO

BL-1031

Message `<timestamp>, [BL-1031], <sequence-number>,, CRITICAL, <system-name>, Link timeout in internal port (slot <Slot number>, port <Port number>) resulted in blade fault. Use slotpoweroff/slotpoweron to recover the blade.`

Probable Cause Indicates that link timeout occurred in one of the backend internal ports.

Recommended Action Power cycle the blade or run the **slotPowerOff** and **slotPowerOn** commands.

Severity CRITICAL

BL-1032

Message `<timestamp>, [BL-1032], <sequence-number>,, CRITICAL, <system-name>, (slot <slot number>,bitmap 0x<object control flags(bitmap)>) ports never came up ONLINE (reason <reason for port disable>, state <status of the blade>). Disabling slot.`

Probable Cause Indicates that back-end (non-user) ports have not come ONLINE within time limit.

Recommended Action Restart or power cycle the blade. Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. If the message persists, replace the blade.

Refer to the *Fabric OS Command Reference* for more information on the **systemVerification** command.

Severity CRITICAL

BL-1033

Message `<timestamp>, [BL-1033], <sequence-number>,, CRITICAL, <system-name>, (slot <slot number>,bitmap 0x<object control flags(bitmap)>) No disable acknowledgment from ports (state <status of the blade>). Disabling slot.`

Probable Cause Indicates that the system has timed out while waiting for disable messages from the user ports after disabling the ports.

Recommended Action Restart or power cycle the blade. Run the **systemVerification** command to verify that the blade does not have hardware problems. Run the **diagPost** command to ensure that Power-On Self-Test (POST) is enabled. If the message persists, replace the blade.

Refer to the *Fabric OS Command Reference* for more information on the **systemVerification** command.

Severity CRITICAL

BL-1034

Message

```
<timestamp>, [BL-1034], <sequence-number>,, INFO, <system-name>, Slot <slot
number> FC Initialization completed.
```

Probable Cause Indicates that the slot has completed initializing Fibre Channel (FC) ports.

Recommended Action No action is required.

Severity INFO

BL-1035

Message

```
<timestamp>, [BL-1035], <sequence-number>,, INFO, <system-name>, Slot <slot
number> iSCSI port <iscsi port number> Initialization completed.
```

Probable Cause Indicates that the slot has completed initializing the specified iSCSI port.

Recommended Action No action is required.

Severity INFO

BL-1036

Message

```
<timestamp>, [BL-1036], <sequence-number>,, CRITICAL, <system-name>, Faulting 8G
blade in slot = <slot number> due to incompatible stag mode. All EX/VEX ports must
be disabled in order to enable the 8G blade in the chassis.
```

Probable Cause Indicates that the FOS 6.0, 8G blade with legacy mode (EX_port having stag) will be disabled.

Recommended Action Disable all EX/VEX ports and perform a **slotpoweroff** or **slotpoweron** operation on the 8G blade. Also, all EX/VEX ports can be re-enabled now.

Severity CRITICAL

BL-1037

Message `<timestamp>, [BL-1037], <sequence-number>,, CRITICAL, <system-name>, Faulting chip in slot = <slot number>, miniS = <miniS number>, port = <port number> due to BE/BI port fault.`

Probable Cause Indicates a fault on the chip and that all ports on the chip have been disabled.

Recommended Action No action is required.

Severity CRITICAL

BL-1038

Message `<timestamp>, [BL-1038], <sequence-number>,, CRITICAL, <system-name>, Inconsistent FPGA image version detected, please restart the switch for recovery.`

Probable Cause Indicates that the FPGA image version is incompatible with the software version.

Recommended Action Restart the switch. If the message persists, replace the switch.

Severity CRITICAL

BL-1039

Message `<timestamp>, [BL-1039], <sequence-number>,, CRITICAL, <system-name>, Inconsistent FPGA image version detected, faulting the blade in slot <slot number>.`

Probable Cause Indicates that the FPGA image version is incompatible with the software version.

Recommended Action Power cycle the blade. If the message persists, replace the blade.

Severity CRITICAL

BL-1041

Message `<timestamp>, [BL-1041], <sequence-number>,, CRITICAL, <system-name>, Dynamic area mode is enabled on default switch, Faulting the blade w/ ID <Blade ID of blade that has the mini SFP+ that does not support it> in slot <slot number> as it does not support this mode.`

Probable Cause Indicates that the blade does not support dynamic area mode on default switch.

Recommended Action Turn off the dynamic area mode through Configure CLI.

Severity CRITICAL

BL-1045

Message `<timestamp>, [BL-1045], <sequence-number>,, ERROR, <system-name>, mini SFP+ (SN: <mini SFP+ serial number>) is only supported in certain high port count blades, not blade in slot <slot number of blade that has the mini SFP+> w/ ID <Blade ID of blade that has the mini SFP+ that does not support it>.`

Probable Cause Indicates that the mini (form factor) SFP+ is supported only by a certain type of blade (FC8-64), but it can be inserted in other blades.

Recommended Action Replace the mini SFP+ with an SFP or SFP+.

Severity ERROR

BL-1046

Message `<timestamp>, [BL-1046], <sequence-number>,, ERROR, <system-name>, <Slot number of blade that has the SFP> error on SFP in Slot <Port number into which the SFP is inserted>/Port <The type of error "checksum" or "data access" for general problems accessing the i2c accessible data> (<A detailed error code>). Try reseating or replacing it.`

Probable Cause Indicates the checksum in an area on the SFP does not match with the computed one or there is problem accessing the data.

Recommended Action Try reseating the SFP, if problem persists replace it.

Severity ERROR

Chapter

BLL System Messages

8

BLL-1000

Message

```
<timestamp>, [BLL-1000], <sequence-number>, FFDC, CRITICAL, <system-name>, ASIC
driver detected Slot <slot number> port <port number> as faulty (reason: <reason>)
```

Probable Cause

Indicates a blade regulation problem was reported on the specified *slot number*. The blade is faulted.

The possible reason codes are as follows:

- 1 = Available buffer overflow
- 2 = Backend port buffer timeout
- 3 = Backend port got shut down
- 4 = Embedded port buffer timeout
- 5 = Excessive busy mini buffer
- 6 = Excessive RCC VC on E_Port
- 7 = Excessive RCC VC on FL_Port
- 8 = Fail detection buffer tag error
- 9 = Fail detection TX parity error
- 10 = EPI CMEM interrupt error
- 11 = CMI interrupt error
- 12 = Interrupt overrun
- 13 = FDET interrupt
- 14 = Interrupt suspended
- 15 = Filter LISTD error
- 16 = Unknown filter LIST error
- 17 = Wait for LPC open state
- 18 = Wait for Old port state
- 19 = Wait for Open init state
- 20 = TX parity error
- 21 = RAM parity error
- 22 = BISR or RAMINIT error

Recommended Action

Make sure the blade is seated correctly. If the blade is seated correctly, restart or power cycle the blade. Run the **systemVerification** command to verify that the blade does not have any hardware problems. To run this command root access is required. Refer to the *Fabric OS Command Reference* for more information on this command. If the message persists, replace the blade.

8 BLL-1000

Severity CRITICAL

Chapter

BLS System Messages

9

BLS-1000

Message `<timestamp>, [BLS-1000], <sequence-number>,, ERROR, <system-name>, <command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>.`

Probable Cause Indicates that the hardware is not responding to a command request, possibly because it is busy.

Recommended Action Retry the command.

Severity ERROR

BLS-1001

Message `<timestamp>, [BLS-1001], <sequence-number>,, CRITICAL, <system-name>, FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.`

Probable Cause Indicates that a FIPS failure has occurred and requires faulting the blade or switch.

Recommended Action Retry the command.

Severity CRITICAL

BLS-1002

Message `<timestamp>, [BLS-1002], <sequence-number>,, INFO, <system-name>, An IPsec/IKE policy was added.`

Probable Cause Indicates that an IPsec or IKE policy was added and the configuration file was updated.

Recommended Action No action is required.

Severity INFO

BLS-1003

Message `<timestamp>, [BLS-1003], <sequence-number>,, INFO, <system-name>, An IPsec/IKE policy was deleted.`

Probable Cause Indicates that an IPsec or IKE policy was deleted and the configuration file was updated.

Recommended Action No action is required.

Severity INFO

BLS-1004

Message
```
<timestamp>, [BLS-1004], <sequence-number>,, INFO, <system-name>, Tape Read
Pipelining is being disabled slot <slot number> port <user port index> tunnel <The
configured tunnel ID (0-7)>.
```

Probable Cause Indicates that the FOS version on the remote end of the tunnel does not support the Tape Read Pipelining feature.

Recommended Action No action is required.

Severity INFO

BLS-1005

Message
```
<timestamp>, [BLS-1005], <sequence-number>,, ERROR, <system-name>, S<slot
number>,P<user port index><blade index> [OID 0x<port OID>8x]: <string name of GE>:
port faulted due to SFP validation failure. Please check if the SFP is valid for
the configuration.
```

Probable Cause Indicates a deteriorated SFP, an incompatible SFP pair, or a faulty cable between the peer ports.

Recommended Action Ensure that you are using compatible SFPs on the peer ports. Verify whether the SFPs have deteriorated and the Fibre Channel cable is faulty. Replace the SFPs or cable, if necessary.

Severity ERROR

Chapter

BM System Messages

10

BM-1001

Message `<timestamp>, [BM-1001], <sequence-number>,, ERROR, <system-name>, BM protocol version <Protocol version> in slot <Slot number>.`

Probable Cause Indicates that the firmware running on the control processor (CP) cannot communicate with the application processor (AP) blade in the indicated slot and determine the AP blade's firmware version.

- The CP blade is running a later version of firmware than the AP blade.
- The CP blade is running an earlier version of firmware than the AP blade.

Recommended Action The problem can be corrected by changing the firmware version on either the control processor (CP) or on the application processor (AP) blade. You can modify the firmware version on the CP blade by using the **firmwareDownload** command. Refer to the release notes to determine whether a non-disruptive firmware download is supported between the revisions. Because the AP and CP blades cannot communicate, it is not possible to load new firmware on the AP blade. If needed, send the AP blade back to the factory for a firmware update.

Severity ERROR

BM-1002

Message `<timestamp>, [BM-1002], <sequence-number>,, INFO, <system-name>, Connection established between CP and blade in slot <Slot number>.`

Probable Cause Indicates the control processor (CP) has established a connection to the blade processor (BP) and can communicate.

Recommended Action No action is required as this is the expected behavior.

Severity INFO

BM-1003

Message `<timestamp>, [BM-1003], <sequence-number>,FFDC, WARNING, <system-name>, Failed to establish connection between CP and blade in slot <Slot number>. Faulting blade.`

Probable Cause Indicates the control processor (CP) could not establish a connection with the blade processor (BP) to communicate.

Recommended Action Use the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade.

Severity WARNING

BM-1004

Message
```
<timestamp>, [BM-1004], <sequence-number>,, INFO, <system-name>, Blade firmware
<Blade firmware> on slot <Slot> is not consistent with system firmware <System
firmware>. Auto-leveling blade firmware to match system firmware.
```

Probable Cause Indicates the policy of the specified blade is to auto-level the blade firmware to the system firmware. The reason for the inconsistency may be due to either of the following reasons:

- Blade firmware was detected to be different from the control processor (CP) firmware due to a firmware upgrade.
- The blade was just inserted and had a different version of the firmware loaded.

Recommended Action No action is required. The blade will automatically download the updated firmware.

Severity INFO

BM-1005

Message
```
<timestamp>, [BM-1005], <sequence-number>,, WARNING, <system-name>,
Firmwaredownload timed-out for blade in slot <Slot>. Faulting blade.
```

Probable Cause Indicates the **firmwareDownload** command failed for the blade in the specified slot.

Recommended Action Use the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade. On the Brocade 7500 or 7600, switch off and switch on all primary power to power-cycle the unit.

Severity WARNING

BM-1006

Message
```
<timestamp>, [BM-1006], <sequence-number>,, INFO, <system-name>, Blade is not
configured. Persistently disabling all ports for blade in slot <Slot number>.
```

Probable Cause Indicates the policy of the specified blade is set to persistently disable all ports the first time the blade is detected. The message indicates either of the following:

- The blade was detected in this slot for the first time.
- The blade was configured under a different mode.

Recommended Action Configure the blade so that it will persistently enable the ports.

Severity INFO

BM-1007

Message `<timestamp>, [BM-1007], <sequence-number>,, INFO, <system-name>, If set, clear EX/VEX/FC Fastwrite configuration for all ports for blade in slot <Slot number>.`

Probable Cause Indicates the specified blade was detected for the first time after an FR4-18i was previously configured in the same slot. The new blade requires the specified port configurations to be cleared.

Recommended Action No action is required. The blade ports are cleared automatically.

Severity INFO

BM-1008

Message `<timestamp>, [BM-1008], <sequence-number>,, WARNING, <system-name>, Download of blade firmware failed for blade in slot <slot>. Reissue firmwaredownload to recover.`

Probable Cause Indicates the automatic firmware upgrade on the blade has failed, because the blade firmware version was detected to be different from the control processor (CP) firmware version due to a firmware upgrade.

Recommended Action Issue the **firmwareDownload** command to recover the blade.

Severity WARNING

BM-1009

Message `<timestamp>, [BM-1009], <sequence-number>,, WARNING, <system-name>, Firmwaredownload timed-out for application processor. Faulting switch.`

Probable Cause Indicates the **firmwareDownload** on the application processor (AP) blade failed.

Recommended Action Use the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade. On the Brocade 7500 or 7600, switch off and switch on all primary power in order to power-cycle the unit.

Severity WARNING

BM-1010

Message `<timestamp>, [BM-1010], <sequence-number>,, INFO, <system-name>, Resetting port configuration and linkcost for all ports for blade in slot <Slot number>.`

Probable Cause Indicates the specified blade was detected for the first time after an FC10-6 was previously configured in the same slot. The new blade requires resetting the port configuration and linkcost.

Recommended Action No action is required. The blade ports are cleared automatically.

Severity INFO

BM-1053

Message `<timestamp>, [BM-1053], <sequence-number>,, WARNING, <system-name>, Failed to establish connection between CP and Application Processor. Faulting switch.`

Probable Cause Indicates the control processor (CP) could not establish a connection with the application processor to communicate.

Recommended Action On the Brocade 7500 or 7600, switch off and switch on all the primary power to power-cycle the unit.

Severity WARNING

BM-1054

Message `<timestamp>, [BM-1054], <sequence-number>,, INFO, <system-name>, AP firmware <Blade firmware> is not consistent with system firmware <System firmware>. Auto-leveling AP firmware to match system firmware.`

Probable Cause Indicates the policy of the specified blade is set to auto-level the blade firmware to the system firmware. This may be due to one of the following reasons:

- Blade firmware was detected to be different from control processor (CP) firmware due to a firmware upgrade.
- The blade was just inserted and had a different version of the firmware loaded.

Recommended Action No action is required. The blade will automatically download the updated firmware.

Severity INFO

BM-1055

Message `<timestamp>, [BM-1055], <sequence-number>,, WARNING, <system-name>, Firmwaredownload timed-out for AP. Faulting switch.`

Probable Cause Indicates the **firmwareDownload** command on the application processor (AP) blade has failed.

Recommended Action Use the **slotPowerOff** and **slotPowerOn** commands or reseat the affected blade. On the Brocade DCX, 7500 or 7600, switch off and switch on all primary power in order to power-cycle the unit.

Severity WARNING

BM-1056

Message `<timestamp>, [BM-1056], <sequence-number>,, INFO, <system-name>, AP is not configured. Persistently disabling all ports on the switch.`

Probable Cause Indicates the policy of the specified switch is to persistently disable all ports the first time the AP is detected. This may be caused by one of the following:

- The AP was detected for the first time on this switch.
- The switch was configured under a different mode.

Recommended Action Configure the switch to persistently enable all ports.

Severity INFO

BM-1058

Message `<timestamp>, [BM-1058], <sequence-number>,, WARNING, <system-name>, Download of AP firmware failed for the switch. Reissue firmwaredownload to recover.`

Probable Cause Indicates the automatic firmware upgrade on the application processor (AP) has failed, because the firmware version running on the AP was detected to be different from the system firmware because of a firmware upgrade.

Recommended Action Issue the **firmwareDownload** command to recover the AP.

Severity WARNING

Chapter

C2 System Messages

11

C2-1001

Message `<timestamp>, [C2-1001], <sequence-number>,, ERROR, <system-name>, Port <port number> port faulted due to SFP validation failure. Please check if the SFP is valid for the configuration.`

Probable Cause Indicates a deteriorated SFP, an incompatible SFP pair, or a faulty cable between the peer ports.

Recommended Action Verify that you are using compatible SFPs on the peer ports. Verify that the SFPs have not deteriorated and the Fibre Channel cable is not faulty. Replace SFPs or cable if necessary.

Severity ERROR

C2-1002

Message `<timestamp>, [C2-1002], <sequence-number>,, ERROR, <system-name>, Port <port number> chip faulted due to an internal error.`

Probable Cause Internal error. All the ports on the blade or switch will be disrupted.

Recommended Action For a bladed system, perform **slotpoweroff** and **slotpoweron** operations on the blade to recover the system. For a non-bladed system, perform fastboot on the switch to recover the system.

Severity ERROR

C2-1004

Message `<timestamp>, [C2-1004], <sequence-number>,, ERROR, <system-name>, <slot number>,<chip index>: Invalid DMA ch pointer, chan:<Channel number>, good_addr:<Good address> bad_addr:<Bad address>.`

Probable Cause Indicates an internal error in the Application-Specific Integrated Circuit (ASIC) hardware that may degrade data traffic.

Recommended Action Whenever this error is observed, restart the system at the next maintenance window. If the problem persists, replace the blade.

Severity ERROR

C2-1006

Message `Message <timestamp>, [C2-1006], <sequence-number>,, WARNING, <system-name>, <slot number>,<chip index>: Internal link errors reported, no hardware faults identified, continuing monitoring: fault1:<fault1_cnt>, fault2:<fault2_cnt> thresh1:0x<threshold_used>.`

Probable Cause Indicates a warning that some internal link errors have been detected. These can be normal in an active running system.

The system will now automatically start a more detailed monitoring of internal hardware reported errors. There is no action required by the user at this time. If any actual hardware failures are detected, a C2-1010 log will be generated identifying the failing FRU.

Recommended Action No action is required.

Severity WARNING

C2-1007

Message `Message <timestamp>, [C2-1007], <sequence-number>,, WARNING, <system-name>, S <slot number>, P <port number>(<blade port number>): best effort QOS will be turned off at next port state change as it is not supported under this configuration.`

Probable Cause Indicates QoS will be turned off automatically at the next port state change since best effort is no longer supported on a 4G platform or 8G platform long distance port.

Recommended Action No action is required.

Severity WARNING

C2-1008

Message `Message <timestamp>, [C2-1008], <sequence-number>,, WARNING, <system-name>, <slot number>, <port number><blade port number>: QOS overwrites portcfglongdistance vc_translation_link_init.  ARB will be used on the link.`

Probable Cause Indicates QoS overwrites the portcfglongdistance vc_translation_link_init 0 choice. ARB will be used on the link.

Recommended Action No action is required.

Severity WARNING

C2-1009

Message Message <timestamp>, [C2-1009], <sequence-number>,, WARNING, <system-name>, <slot number>, <port number><blade port number>: portcfglongdistance vc_translation_link_init = 1 overwrites fill word IDLE. ARB will be used on the link.

Probable Cause Indicates portcfglongdistance vc_translation_link_init 1 overwrites fill word IDLE. ARB will be used on the link.

Recommended Action No action is required.

Severity WARNING

C2-1010

Message Message <timestamp>, [C2-1010], <sequence-number>,, CRITICAL, <system-name>, S <slot number>, C <chip index>: Internal monitoring has identified suspect hardware, blade may need to be reset or replaced: fault1:<fault1_cnt>, fault2:<fault2_cnt> th2:0x<threshold_used>.

Probable Cause Indicates above normal errors observed in hardware that may or may not impact data traffic.

Recommended Action Whenever this error is observed persistently, power cycle the faulted blade. If the problem persists, replace the blade.

Severity CRITICAL

C2-1011

Message Message <timestamp>, [C2-1011], <sequence-number>,, WARNING, <system-name>, S <slot number>, P <port number><blade port number>: Primitive received with Encoding errors, do AL_RESET.

Probable Cause Indicates encoding errors on the internal links.

Recommended Action This error can cause CRC errors or frame loss. If the error is observed continuously, power cycle the affected blade first. If the problem persists, check the backplane and/or replace the blade.

Severity WARNING

11 C2-1011

Chapter

CDR System Messages

12

CDR-1001

Message `<timestamp>, [CDR-1001], <sequence-number>,, ERROR, <system-name>, Port <port number> port fault. Please change the SFP or check cable`

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP), an incompatible SFP pair, a faulty cable between peer ports, or that the port speed configuration does not match the capability of the SFP.

Recommended Action Ensure that you are using compatible SFPs on the peer ports.

Verify whether the SFPs have deteriorated or the Fibre Channel cable is faulty. Replace the SFPs or cable, if necessary.

Severity ERROR

CDR-1002

Message `<timestamp>, [CDR-1002], <sequence-number>, FFDC, ERROR, <system-name>, Port <port number> chip faulted due to internal error.`

Probable Cause Indicates an internal error.

Recommended Action For a bladed system, execute the **slotPowerOff** and **slotPowerOn** commands on the blade to recover the system. For a non-bladed system, perform **fastBoot** command on the switch to recover the system.

Severity ERROR

CDR-1003

Message `<timestamp>, [CDR-1003], <sequence-number>, FFDC, CRITICAL, <system-name>, <slot number>, <chip index> HW ASIC chip error type =0<chip error type>`

Probable Cause Indicates an internal error in the application specific integrated circuit (ASIC) hardware that may degrade data traffic.

Recommended Action Whenever this error occurs, restart the system at the next maintenance window. If the problem persists, replace the blade.

Severity CRITICAL

CDR-1004

Message `<timestamp>, [CDR-1004], <sequence-number>, FFDC, ERROR, <system-name>, <slot number>, <chip index>: invalid DMA ch pointer, chan:<Channel number>, good_addr:0x<Good address>, bad_addr:0x<Bad address>.`

Probable Cause Indicates an internal error in the application specific integrated circuit (ASIC) hardware that may degrade data traffic.

Recommended Action Whenever this error occurs, restart the system at the next maintenance window. If the problem persists, replace the blade.

Severity ERROR

CDR-1005

Message `<timestamp>, [CDR-1005], <sequence-number>,, WARNING, <system-name>, <slot number>, <port number><blade port number>: at next port state change, best effort QOS will be turned off automatically due to best effort is no longer supported under this configuration.`

Probable Cause Indicates QoS will be turned off automatically at the next port state change because best effort is no longer supported on a 4G platform or 8G platform long distance port.

Recommended Action No action is required.

Severity WARNING

CDR-1006

Message `<timestamp>, [CDR-1006], <sequence-number>,, WARNING, <system-name>, <slot number>, <port number><blade port number>: QOS overwrites portcfglongdistance vc_translation_link_init. ARB will be used on the link.`

Probable Cause Indicates QoS overwrites the portcfglongdistance vc_translation_link_init 0 choice. ARB will be used on the link.

Recommended Action No action is required.

Severity WARNING

Chapter

CEE CONFIG System Messages

13

CCFG-1001

Message `<timestamp>, [CCFG-1001], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module>, rc = <error>.`

Probable Cause Indicates that initialization of a module within the Converged Enhanced Ethernet (CEE) configuration management daemon has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

CCFG-1002

Message `<timestamp>, [CCFG-1002], <sequence-number>,, INFO, <system-name>, Started loading CEE system configuration.`

Probable Cause Indicates that the Converged Enhanced Ethernet (CEE) system configuration has started loading.

Recommended Action No action is required.

Severity INFO

CCFG-1003

Message `<timestamp>, [CCFG-1003], <sequence-number>,, INFO, <system-name>, System is ready to accept CEE user commands.`

Probable Cause Indicates that the Converged Enhanced Ethernet (CEE) shell is ready to accept configuration commands from the user.

Recommended Action No action is required.

Severity INFO

CCFG-1004

Message `<timestamp>, [CCFG-1004], <sequence-number>,, ERROR, <system-name>, Configuration replay failed due to missing system startup configuration.`

Probable Cause Indicates that the startup configuration has been moved or deleted, hence replaying the system configuration has failed.

Recommended Action Use the **copy file startup-config** command to restore the startup configuration from any backup retrieved on the server.

Severity ERROR

CCFG-1005

Message `<timestamp>, [CCFG-1005], <sequence-number>,, INFO, <system-name>, Startup configuration is updated.`

Probable Cause Indicates that the startup configuration has been updated by the user.

Recommended Action No action is required.

Severity INFO

CCFG-1006

Message `<timestamp>, [CCFG-1006], <sequence-number>,, INFO, <system-name>, Current system running configuration is updated.`

Probable Cause Indicates that the current running configuration has been updated.

Recommended Action No action is required.

Severity INFO

CCFG-1007

Message `<timestamp>, [CCFG-1007], <sequence-number>,, INFO, <system-name>, startup configuration is erased.`

Probable Cause Indicates that the startup configuration has been moved or deleted.

Recommended Action No action is required.

Severity INFO

CCFG-1008

Message `<timestamp>, [CCFG-1008], <sequence-number>,, ERROR, <system-name>, CMSH init failed: <message>.`

Probable Cause Indicates that the CMSH initialization has failed.

Recommended Action No action is required.

Severity ERROR

CCFG-1009

Message `<timestamp>, [CCFG-1009], <sequence-number>,, INFO, <system-name>, Successfully copied to <destination>.`

Probable Cause Indicates that the file has been successfully copied to the destination.

Recommended Action No action is required.

Severity INFO

CCFG-1010

Message `<timestamp>, [CCFG-1010], <sequence-number>,, INFO, <system-name>, Current system running configuration is updated partially.`

Probable Cause Indicates that the current running configuration has been updated partially.

Recommended Action No action is required.

Severity INFO

CCFG-1011

Message `<timestamp>, [CCFG-1011], <sequence-number>,, WARNING, <system-name>, Linecard configuration mismatch on slot <slot>.`

Probable Cause Indicates that the inserted linecard is different from the pre-configured one.

Recommended Action Remove the incompatible linecard or use **no linecard** command to remove configuration.

Severity WARNING

CCFG-1012

Message `<timestamp>, [CCFG-1012], <sequence-number>,, ERROR, <system-name>, Blade in slot <slot> failed to reach ONLINE state within <timeout> seconds after receiving system ready.`

Probable Cause Indicates that the mentioned slot has failed to reach the Online state within the specified time after system ready event.

Recommended Action Run the **slotpoweroff** command followed by the **slotpoweron** command on the slot to retry bringing the slot online.

Severity ERROR

Chapter

CER System Messages

14

CER-1001

Message `<timestamp>, [CER-1001], <sequence-number>,, ERROR, <system-name>, HA Sync broken, since standby Advanced Performance Tuning module does not support FICON Management Server (FMS).`

Probable Cause Indicates that the high-availability (HA) synchronization between the active and standby control processors (CPs) is broken, because there is downlevel firmware loaded on the standby CP. The standby CP does not support the Advanced Performance Tuning module when the fibre connectivity (FICON) Management Server is enabled.

Recommended Action Run the **firmwareDownload** command to upgrade the firmware on the standby CP.

You can also disable FMS on the active CP.

Severity ERROR

Chapter

CHASSIS System Messages

15

CHASSIS-1002

Message `<timestamp>, [CHASSIS-1002], <sequence-number>,, ERROR, <system-name>, ki_gd_register_action failed with rc =<ret val>.`

Probable Cause Indicates an internal error.

Recommended Action For a bladed system, execute the **slotPowerOff** command and **slotPowerOn** commands on the blade to recover the system. For a non-bladed system, execute the **fastBoot** command on the switch to recover the system.

Severity ERROR

CHASSIS-1003

Message `<timestamp>, [CHASSIS-1003], <sequence-number>,, ERROR, <system-name>, Slot ENABLED but Not Ready during recovery, disabling slot = <slot number> rval = <return value>.`

Probable Cause Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action On a Brocade 24000 or 48000 switch, run the **slotPowerOff** command followed by the **slotPowerOn** command. On a Brocade 7500 or AP7600 switch, reboot or power cycle the switch.

Severity ERROR

CHASSIS-1004

Message `<timestamp>, [CHASSIS-1004], <sequence-number>,, ERROR, <system-name>, Blade attach failed during recovery, disabling slot = <slot number>, rval = <return value>.`

Probable Cause Indicates that a blade has failed during failover or recovery.

Recommended Action On a Brocade 24000 or 48000 switch, run the **slotPowerOff** command followed by the **slotPowerOn** command. On a Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, or AP7600 switch, reboot or power cycle the switch.

Severity ERROR

CHASSIS-1005

Message `<timestamp>, [CHASSIS-1005], <sequence-number>,, ERROR, <system-name>, Diag attach failed during recovery, disabling slot = <slot number>.`

Probable Cause Indicates that the Diag blade attach has failed during failover or recovery.

Recommended Action On a Brocade 24000 or 48000 switch, run the **slotPowerOff** command followed by the **slotPowerOn** command. On a Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, or AP7600 switch, reboot or power cycle the switch.

Severity ERROR

Chapter

CNM System Messages

16

CNM-1001

Message `<timestamp>, [CNM-1001], <sequence-number>,, ERROR, <system-name>, Failed to allocate memory: <function name>.`

Probable Cause Indicates that the specified function failed to allocate memory.

Recommended Action Check memory usage on the switch using the **memShow** command. Restart or power cycle the switch.

Severity ERROR

CNM-1002

Message `<timestamp>, [CNM-1002], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module> rc = <error>.`

Probable Cause Indicates that an initialization of a module within the CNM has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

CNM-1003

Message `<timestamp>, [CNM-1003], <sequence-number>,, WARNING, <system-name>, Crypto device configuration between local switch (<local domain id>) and peer (<peer domain id>) is out of sync. New encryption session is not allowed.`

Probable Cause Indicates that the encryption engine (EE) nodes in the cluster encryption group have different configurations.

Recommended Action Synchronize the configuration in the cluster group using the **cryptodevicecfg** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity WARNING

CNM-1004

Message `<timestamp>, [CNM-1004], <sequence-number>,, INFO, <system-name>, iSCSI service is <status> on the switch.`

Probable Cause Indicates that the Crypto service is enabled or disabled on the switch.

Recommended Action No action is required.

Severity INFO

CNM-1005

Message `<timestamp>, [CNM-1005], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_GRP_LEADER_ELECTED Name [<nodeName>], WWN [<WWn>].`

Probable Cause Indicates that the cluster encryption group (EG) leader is elected.

Recommended Action No action is required.

Severity INFO

CNM-1006

Message `<timestamp>, [CNM-1006], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_NODE_JOIN nodeName [<nodeName>], wwn [<wwn>], ipaddress [<ipAddr>].`

Probable Cause Indicates that the member node has joined.

Recommended Action No action is required.

Severity INFO

CNM-1007

Message `<timestamp>, [CNM-1007], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_GRP_LEADER_FAILED Name [<nodeName>].`

Probable Cause Indicates that the Group Leader has failed.

Recommended Action No action is required.

Severity INFO

CNM-1008

Message `<timestamp>, [CNM-1008], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_NODE_EJECT nodeName [<nodeName>], wwn [<wwn>].`

Probable Cause Indicates that the node is ejected from the encryption group (EG).

Recommended Action No action is required.

Severity INFO

CNM-1009

Message `<timestamp>, [CNM-1009], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_STANDALONE_MODE.`

Probable Cause Indicates that the node is in standalone mode.

Recommended Action No action is required.

Severity INFO

CNM-1010

Message `<timestamp>, [CNM-1010], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_CLUSTER_UDATA_UPDATE cid [<client id>], ulen [<udata len>].`

Probable Cause Indicates the client data update.

Recommended Action No action is required.

Severity INFO

CNM-1011

Message `<timestamp>, [CNM-1011], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_NODE_JOIN_TIMEOUT nodeName [<nodeName>], wwn [<wwn>], ipaddress [<ipAddr>].`

Probable Cause Indicates the node join timeout.

Recommended Action Take the peer node offline, rejoin the node to the encryption group (EG).

Severity INFO

CNM-1012

Message `<timestamp>, [CNM-1012], <sequence-number>,, INFO, <system-name>,Posting event CNM_EVT_EG_DELETED.`

Probable Cause Indicates that the encryption group (EG) is deleted.

Recommended Action No action is required.

Severity INFO

CNM-1013

Message `<timestamp>, [CNM-1013], <sequence-number>,, INFO, <system-name>,Posting event GL Node Split condition, isolating peer GL node <nodeName>.`

Probable Cause Indicates that the encryption group (EG) is split.

Recommended Action No action is required.

Severity INFO

CNM-1014

Message `<timestamp>, [CNM-1014], <sequence-number>,, INFO, <system-name>,Posting event Node Admission Control passed, admitting node [<nodeName>].`

Probable Cause Indicates that the Node Admission Control was successful.

Recommended Action No action is required.

Severity INFO

CNM-1015

Message `<timestamp>, [CNM-1015], <sequence-number>,, INFO, <system-name>,Posting event Potential Cluster Split condition.`

Probable Cause Indicates the posting event of a Potential Cluster Split condition.

Recommended Action No action is required.

Severity INFO

CNM-1016

Message `<timestamp>, [CNM-1016], <sequence-number>,, INFO, <system-name>,Posting event Detected a EG degrade condition.`

Probable Cause Indicates an encryption group (EG) degrade condition.

Recommended Action No action is required.

Severity INFO

CNM-1017

Message `<timestamp>, [CNM-1017], <sequence-number>,, INFO, <system-name>,Got JOIN REQUEST from un-recognized GL node [<rxglname>], configured GL node is [<glname>].`

Probable Cause Indicates a join request was received from an invalid group leader (GL) node.

Recommended Action No action is required.

Severity INFO

CNM-1018

Message `<timestamp>, [CNM-1018], <sequence-number>,, INFO, <system-name>, Got CNM_FSM_EVT_JOIN_REQ when already a member, My assigned name [<nodename>], dropping request.`

Probable Cause Indicates that the node is already a member.

Recommended Action No action is required.

Severity INFO

CNM-1019

Message `<timestamp>, [CNM-1019], <sequence-number>,, INFO, <system-name>, Join Rejected by GL node, fix certificate and later add member node from GL node, or reboot the member node.`

Probable Cause Indicates an invalid member node certificate.

Recommended Action No action is required.

Severity INFO

CNM-1020

Message `<timestamp>, [CNM-1020], <sequence-number>,, INFO, <system-name>, Node Admission Control failed, due to mismatch in certificates, rejecting node [<nodename>].`

Probable Cause Indicates that the Node Admission Control has failed.

Recommended Action No action is required.

Severity INFO

CNM-1021

Message `<timestamp>, [CNM-1021], <sequence-number>,, INFO, <system-name>, Failed to sign the node authentication message, admission control might fail.`

Probable Cause Indicates that the Node Admission Control has failed.

Recommended Action No action is required.

Severity INFO

CNM-1022

Message `<timestamp>, [CNM-1022], <sequence-number>,, INFO, <system-name>, Operation not allowed on GL Node.`

Probable Cause Indicates an operation is not allowed on a group leader (GL) node.

Recommended Action No action is required.

Severity INFO

CNM-1023

Message `<timestamp>, [CNM-1023], <sequence-number>,, INFO, <system-name>, Group Leader node eject is not allowed.`

Probable Cause Indicates an eject operation is not allowed on a group leader (GL) node.

Recommended Action No action is required.

Severity INFO

CNM-1024

Message `<timestamp>, [CNM-1024], <sequence-number>,, INFO, <system-name>, Operation not required on GL node.`

Probable Cause Indicates an operation is not required on a group leader (GL) node.

Recommended Action No action is required.

Severity INFO

CNM-1025

Message `<timestamp>, [CNM-1025], <sequence-number>,, INFO, <system-name>, Operation not allowed, as member is active with the Cluster. Eject member node and retry.`

Probable Cause Indicates an operation is not allowed on a member node.

Recommended Action No action is required.

Severity INFO

CNM-1026

Message `<timestamp>, [CNM-1026], <sequence-number>,, INFO, <system-name>, Received HBT Message with version mismatch, Received Hdr version <rxhdrver> Expected Hdr version <exphdrver> Node <wwn>.`

Probable Cause Indicates that a version mismatch has occurred.

Recommended Action Upgrade the firmware or delete the Node from the encryption group (EG).

Severity INFO

CNM-1027

Message `<timestamp>, [CNM-1027], <sequence-number>,, INFO, <system-name>, Received HBT from Non-Group Member Node [<wwn>].`

Probable Cause Indicates an operation is not allowed on a non-group member node.

Recommended Action No action is required.

Severity INFO

CNM-1028

Message `<timestamp>, [CNM-1028], <sequence-number>,, INFO, <system-name>, Certfile <cfname> already exists. No need to sync up.`

Probable Cause Indicates that the certificate file for the node already exists.

Recommended Action No action is required.

Severity INFO

CNM-1029

Message `<timestamp>, [CNM-1029], <sequence-number>,, WARNING, <system-name>, Certfile <cfname> content does not match the cert sent by GL.`

Probable Cause Indicates that the contents of the node's certificate file is different from the certificate file sent by the group leader (GL) node.

Recommended Action No action is required.

Severity WARNING

CNM-1030

Message `<timestamp>, [CNM-1030], <sequence-number>,, WARNING, <system-name>, Certfile <cfname> read less number of bytes <nbytes>.`

Probable Cause Indicates that the read operation of the certificate file returned a fewer number of bytes than expected.

Recommended Action No action is required.

Severity WARNING

CNM-1031

Message `<timestamp>, [CNM-1031], <sequence-number>,, WARNING, <system-name>, Certfile <cfname> open failed with errno <errno>.`

Probable Cause Indicates that an attempt to open the certificate file has failed.

Recommended Action No action is required.

Severity WARNING

CNM-1032

Message `<timestamp>, [CNM-1032], <sequence-number>,, WARNING, <system-name>, Certfile <cfname> size <fsize> does not match cert file size <len> sent by GL`

Probable Cause Indicates that there is a size mismatch between a node's certificate file and the certificate file received from the group leader.

Recommended Action No action is required.

Severity WARNING

CNM-1033

Message `<timestamp>, [CNM-1033], <sequence-number>,, WARNING, <system-name>, Some of the defined nodes in the Encryption Group are not ONLINE. Encryption Group is in degraded state.`

Probable Cause Indicates that the cluster is in a degraded state.

Recommended Action No action is required.

Severity WARNING

CNM-1034

Message `<timestamp>, [CNM-1034], <sequence-number>,, INFO, <system-name>, All the defined nodes in the Encryption Group are ONLINE. Cluster is in converged state.`

Probable Cause Indicates that the cluster is in a converged state.

Recommended Action No action is required.

Severity INFO

CNM-1035

Message `<timestamp>, [CNM-1035], <sequence-number>,, WARNING, <system-name>, Cluster is in degraded state. Posting degrade event.`

Probable Cause Indicates an event is being posted to indicate that the cluster is in a degraded state.

Recommended Action No action is required.

Severity WARNING

CNM-1036

Message `<timestamp>, [CNM-1036], <sequence-number>,, INFO, <system-name>, All the active nodes of the cluster are in ONLINE state. Posting converged event.`

Probable Cause Indicates an event is being posted to indicate that the cluster is in a converged state.

Recommended Action No action is required.

Severity INFO

CNM-1037

Message `<timestamp>, [CNM-1037], <sequence-number>,, INFO, <system-name>, Split-Brain Arbitration lost!, minority GL Node, remote:local [<rem_count>:<loc_gl_ncount>].`

Probable Cause Indicates that split arbitration is lost.

Recommended Action No action is required.

Severity INFO

CNM-1038

Message `<timestamp>, [CNM-1038], <sequence-number>,, INFO, <system-name>, Split-Brain Arbitration won, majority GL Node, remote:local [<rem_count>:<loc_gl_ncount>].`

Probable Cause Indicates that split arbitration is won.

Recommended Action No action is required.

Severity INFO

CNM-1039

Message `<timestamp>, [CNM-1039], <sequence-number>,, INFO, <system-name>, Split-Brain Arbitration lost!, Minority WWN/GL Node, remote_wwn:local_wwn <wbuf>.`

Probable Cause Indicates that split arbitration is lost.

Recommended Action No action is required.

Severity INFO

CNM-1040

Message `<timestamp>, [CNM-1040], <sequence-number>,, INFO, <system-name>, Split-Brain Arbitration won, Majority WWN/GL Node, remote_wwn:local_wwn <wwn>.`

Probable Cause Indicates that split arbitration is won.

Recommended Action No action is required.

Severity INFO

CNM-1041

Message `<timestamp>, [CNM-1041], <sequence-number>,, INFO, <system-name>, Updating persistent Cluster DB, please avoid powering off the switch.`

Probable Cause Indicates the system is updating the persistent database.

Recommended Action No action is required.

Severity INFO

CNM-1042

Message `<timestamp>, [CNM-1042], <sequence-number>,, INFO, <system-name>, Done, updating persistent Cluster DB.`

Probable Cause Indicates that the update of the persistent database is complete.

Recommended Action No action is required.

Severity INFO

CNM-1043

Message `<timestamp>, [CNM-1043], <sequence-number>,, ERROR, <system-name>, Received HBT from undefined node IpAddress [<ip>], WWN [<wwn>]. Possible configuration error.`

Probable Cause Indicates that the remote node's WWN might be changed.

Recommended Action No action is required.

Severity ERROR

CNM-1044

Message `<timestamp>, [CNM-1044], <sequence-number>,, ERROR, <system-name>, Cluster Create Failed as the Certificate files not found, Please do the initnode.`

Probable Cause Indicates that the initnode is not invoked.

Recommended Action No action is required.

Severity ERROR

CNM-1045

Message `<timestamp>, [CNM-1045], <sequence-number>,, ERROR, <system-name>, Member node <wwn> is having dual IP stack.Registering member node with dual IP in an EG with only IPV6 is not allowed.`

Probable Cause Indicates that the member node with a dual IP stack was registered with an IPV6 encryption group (EG).

Recommended Action No action is required.

Severity ERROR

CNM-1046

Message `<timestamp>, [CNM-1046], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_NODE_LEAVE nodeName <nodeName>, wwn <wwn>.`

Probable Cause Indicates that the node has decided to leave the encryption group (EG).

Recommended Action No action is required.

Severity INFO

CNM-1047

Message `<timestamp>, [CNM-1047], <sequence-number>,, INFO, <system-name>, Network Interface to Remote Node <ip> is <string>.`

Probable Cause Indicates that the status of the network interface is UP or DOWN.

Recommended Action No action is required.

Severity INFO

CNM-1048

Message `<timestamp>, [CNM-1048], <sequence-number>,, INFO, <system-name>, Posting <string>.`

Probable Cause Indicates the event that is posted.

Recommended Action No action is required.

Severity INFO

CNM-1049

Message `<timestamp>, [CNM-1049], <sequence-number>,, ERROR, <system-name>, Failed to define node, Node Name <string>.`

Probable Cause Indicates the system failed to define the node object.

Recommended Action No action is required.

Severity ERROR

CNM-1050

Message `<timestamp>, [CNM-1050], <sequence-number>,, ERROR, <system-name>, Node Admission Control failed due to mismatch in Access Gateway Daemon (AGD) mode settings, rejecting node <nodename>.`

Probable Cause Indicates mode mismatch between the switches like the Access Gateway mode mismatch.

Recommended Action No action is required.

Severity ERROR

CNM-1051

Message `<timestamp>, [CNM-1051], <sequence-number>,, ERROR, <system-name>, Join Rejected by GL Node due to Access Gateway Daemon mode mismatch, ensure mode settings are same across all nodes in EG.`

Probable Cause Indicates mode mismatch between the switches like the Access Gateway mode mismatch.

Recommended Action No action is required.

Severity ERROR

CNM-1052

Message `<timestamp>, [CNM-1052], <sequence-number>,, ERROR, <system-name>, Member node registered with another Encryption Group. To proceed eject the member node <nodename> from other EG.`

Probable Cause Indicates that the member node is registered with another encryption group (EG).

Recommended Action No action is required.

Severity ERROR

CNM-1053

Message `<timestamp>, [CNM-1053], <sequence-number>,, ERROR, <system-name>, Node is already a registered member of another EG. First eject the current node <nodename> from the existing EG and then try.`

Probable Cause Indicates that the node is already a registered member of another encryption group (EG).

Recommended Action No action is required.

Severity ERROR

CNM-1054

Message `<timestamp>, [CNM-1054], <sequence-number>,, INFO, <system-name>, Encryption Group database state <state> with node ip <node>, wwn <wwn>.`

Probable Cause Indicates the status of the cluster database.

Recommended Action No action is required.

Severity INFO

CNM-1055

Message `<timestamp>, [CNM-1055], <sequence-number>,, INFO, <system-name>, Got CNM_FSM_EVT_JOIN_REQ when already a member from same GL node, rejoining EG with GL <glname>.`

Probable Cause Indicates the node is rejoining the encryption group (EG).

Recommended Action No action is required.

Severity INFO

CNM-1056

Message `<timestamp>, [CNM-1056], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_EE_INITIALIZING Slot <slot>, Wwn <wwn>, IP <ip>, flags <flags>.`

Probable Cause Indicates that the encryption engine (EE) is added into the encryption group (EG).

Recommended Action No action is required.

Severity INFO

CNM-1057

Message `<timestamp>, [CNM-1057], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_ONLINE Slot <slot>, Wwn <wwn>, IP <ip>, flags <flags>.`

Probable Cause Indicates that the encryption engine (EE) is online in the encryption group (EG).

Recommended Action No action is required.

Severity INFO

CNM-1058

Message `<timestamp>, [CNM-1058], <sequence-number>,, INFO, <system-name>, Posting event CNM_EVT_OFFLINE Slot <slot>, Wwn <wwn>, IP <ip>, flags <flags>.`

Probable Cause Indicates that the encryption engine (EE) is removed from the encryption group (EG).

Recommended Action No action is required.

Severity INFO

CNM-1059

Message `<timestamp>, [CNM-1059], <sequence-number>,, INFO, <system-name>, Local Node CP certificate pair mismatch detected, re-initialize the node.`

Probable Cause Indicates that the certificate pair is mismatched.

Recommended Action No action is required.

Severity INFO

CNM-1060

Message `<timestamp>, [CNM-1060], <sequence-number>,, INFO, <system-name>, Local Node CP certificate pair mismatch detected.`

Probable Cause Indicates that the certificate pair is matched.

Recommended Action No action is required.

Severity INFO

CNM-1061

Message `<timestamp>, [CNM-1061], <sequence-number>,, INFO, <system-name>, IP of the switch changed from [<my_ip>] to [<new_ip>].`

Probable Cause Indicates that the switch IP has changed.

Recommended Action No action is required.

Severity INFO

CNM-1062

Message `<timestamp>, [CNM-1062], <sequence-number>,, INFO, <system-name>, Copied certificate to [<ofname>] due to change in IP.`

Probable Cause Indicates that the certificate was copied to the file with new IP name.

Recommended Action No action is required.

Severity INFO

CNM-3001

Message `<timestamp>, [CNM-3001], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: encryption group \<encryptiongroupname>\ created.`

Probable Cause Indicates an encryption group was created.

Recommended Action No action is required.

Severity INFO

CNM-3002

Message `<timestamp>, [CNM-3002], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: encryption group deleted.`

Probable Cause Indicates an encryption group was deleted.

Recommended Action No action is required.

Severity INFO

CNM-3003

Message `<timestamp>, [CNM-3003],<sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Membernode \<membernodeWWN>\ added to encryption group.`

Probable Cause Indicates a member node was added to an encryption group.

Recommended Action No action is required.

Severity INFO

CNM-3004

Message `<timestamp>, [CNM-3004], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Membernode \<membernodeWWN>\ ejected from encryption group.`

Probable Cause Indicates a member node was ejected from an encryption group.

Recommended Action No action is required.

Severity INFO

CNM-3005

Message `<timestamp>, [CNM-3005], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Membernode \<membernodeWWN>\ left encryption group.`

Probable Cause Indicates the membernode left an encryption group.

Recommended Action No action is required.

Severity INFO

CNM-3006

Message `<timestamp>, [CNM-3006], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Heartbeat miss count set to <hbmisses>.`

Probable Cause Indicates that the heartbeat miss value was set.

Recommended Action No action is required.

Severity INFO

CNM-3007

Message `<timestamp>, [CNM-3007],<sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Heartbeat timeout set to <hbtimeout>.`

Probable Cause Indicates that the heartbeat timeout value was set.

Recommended Action No action is required.

Severity INFO

CNM-3008

Message `<timestamp>, [CNM-3008], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Routing mode of EE in slot <slot> set to <routingmode>.`

Probable Cause Indicates that the encryption engine (EE) routing mode was set.

Recommended Action No action is required.

Severity INFO

CNM-3009

Message `<timestamp>, [CNM-3009],<sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Membernode <membernodeWWN> registered.`

Probable Cause Indicates a membernode was registered.

Recommended Action No action is required.

Severity INFO

CNM-3010

Message `<timestamp>, [CNM-3010],<sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Membernode <membernodeWWN> unregistered.`

Probable Cause Indicates a membernode was unregistered.

Recommended Action No action is required.

Severity INFO

CNM-3011

Message `<timestamp>, [CNM-3011], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Encryption group synchronized.`

Probable Cause Indicates an encryption group was synchronized.

Recommended Action No action is required.

Severity INFO

CNM-3012

Message `<timestamp>, [CNM-3012], <sequence-number>,, INFO, <system-name>, Deleteing an EG with luns setup for encryption can lead to luns being disabled if Encryption Group name is not preserved (<egname>).`

Probable Cause Indicates that the Encryption Group (EG) was deleted, recreate EG with the same name if luns are setup for encryption.

Recommended Action Preserve EG name when EG is recreated if luns are setup for encryption.

Severity INFO

Chapter

CONF System Messages

17

CONF-1000

Message `<timestamp>, [CONF-1000], <sequence-number>, AUDIT, INFO, <system-name>, configDownload completed successfully. <Info about the parameters and AD>.`

Probable Cause Indicates that the **configDownload** operation was initiated and completed successfully. The statement that follows, message strings, is the description of the classes of configuration parameters that were downloaded. If Admin Domain (AD) is enabled, the AD number is specified in the description.

Recommended Action No action is required.

Severity INFO

CONF-1001

Message `<timestamp>, [CONF-1001], <sequence-number>,, INFO, <system-name>, configUpload completed successfully. <Info about the parameters and AD>.`

Probable Cause Indicates that the **configUpload** operation was initiated and completed successfully. The statement that follows, message strings, is the description of the classes of configuration parameters that were uploaded. If AD is enabled, the AD number is specified in the description.

Recommended Action No action is required.

Severity INFO

CONF-1020

Message `<timestamp>, [CONF-1020], <sequence-number>,, INFO, <system-name>, configDownload not permitted <AD Number if AD is configured on the system>.`

Probable Cause Indicates a **configDownload** operation is not permitted. There are many possible causes.

Recommended Action Check the error log, correct the error and rerun the **configdownload** command.

Severity INFO

CONF-1021

Message `<timestamp>, [CONF-1021], <sequence-number>,, INFO, <system-name>, configUpload not permitted <AD Number if AD is configured on the system>.`

Probable Cause Indicates a **configUpload** operation is not permitted. There are many possible causes.

Recommended Action Check the error log, correct the error and rerun the **configupload** command.

Severity INFO

CONF-1022

Message `<timestamp>, [CONF-1022], <sequence-number>,, WARNING, <system-name>, Downloading configuration without disabling the switch was unsuccessful.`

Probable Cause Indicates an attempt to download the configuration without disabling the switch was unsuccessful because there are one or more parameters that require the switch to be disabled.

Recommended Action Disable the switch using the **switchDisable** command and download the configuration.

Severity WARNING

CONF-1023

Message `<timestamp>, [CONF-1023], <sequence-number>,, INFO, <system-name>, configDownload failed.`

Probable Cause Indicates a **configDownload** operation has failed.

Recommended Action Check the error log, correct the error and rerun the command.

Severity INFO

CONF-1024

Message `<timestamp>, [CONF-1024], <sequence-number>,, INFO, <system-name>, configUpload failed.`

Probable Cause Indicates a **configUpload** operation has failed.

Recommended Action Check the error log, correct the error and rerun the command.

Severity INFO

CONF-1030

Message `<timestamp>, [CONF-1030], <sequence-number>,, WARNING, <system-name>, Configuration database full, data not committed (key:<Key of failed configuration data>.`

Probable Cause Indicates that the previous configuration commands have resulted in a database full condition. Configuration changes associated with the specified key have not been applied.

Recommended Action Use the **configure** command and various other commands to erase configuration parameters that are no longer required. As a last resort, execute the **configDefault** command and reconfigure the system.

Severity WARNING

CONF-1031

Message `<timestamp>, [CONF-1031], <sequence-number>,, INFO, <system-name>, configDefault completed successfully.`

Probable Cause Indicates that the **configDefault** command was initiated and completed successfully.

Recommended Action No action is required.

Severity INFO

CONF-1032

Message `<timestamp>, [CONF-1032], <sequence-number>,, INFO, <system-name>, configRemove completed successfully.`

Probable Cause Indicates that the **configRemove** command was initiated and completed successfully.

Recommended Action No action is required.

Severity INFO

CONF-1040

Message `<timestamp>, [CONF-1040], <sequence-number>,, INFO, <system-name>, configDefault failed.`

Probable Cause Indicates a **configDefault** error has occurred.

Recommended Action Correct the error and try again.

Severity INFO

CONF-1041

Message `<timestamp>, [CONF-1041], <sequence-number>,, INFO, <system-name>, configRemove failed.`

Probable Cause Indicates a **configRemove** error has occurred.

Recommended Action Correct the error and try again.

Severity INFO

CONF-1042

Message `<timestamp>, [CONF-1042], <sequence-number>,, INFO, <system-name>, Fabric Configuration Parameter <parameter> changed to <value>.`

Probable Cause Indicates that the parameter value has been changed.

Recommended Action No action is required.

Severity INFO

CONF-1043

Message `<timestamp>, [CONF-1043], <sequence-number>,, INFO, <system-name>, Fabric Configuration Parameter <parameter> changed to <value>.`

Probable Cause Indicates that the parameter value has been changed.

Recommended Action No action is required.

Severity INFO

Chapter

CTAP System Messages

18

CTAP-1001

Message `<timestamp>, [CTAP-1001], <sequence-number>,, INFO, <system-name>, Key acquisition for <Pool or Container> <Begins or Complete>.`

Probable Cause Indicates that a change in the tape pool database has triggered the key acquisition process for each pool.

Recommended Action Do not start tape backup or restore operations involving tape pools until the process is complete.

Severity INFO

Chapter

CVLC System Messages

19

CVLC-1001

Message `<timestamp>, [CVLC-1001], <sequence-number>,, INFO, <system-name>, <Re-key type (First time encryption/Key expired/Manual)> re-key <Re-key action (started/completed/failed/cancelled)>, LUN SN: <LUN serial number>.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates the First time encryption, Key expired or Manual re-key operation is performed. The operation has been started, completed or cancelled.

Recommended Action No action is required.

Severity INFO

CVLC-1002

Message `<timestamp>, [CVLC-1002], <sequence-number>,, INFO, <system-name>, Tape session <Tape session action (started/cancelled/failed)>.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that a tape session was started or cancelled.

Recommended Action No action is required.

Severity INFO

CVLC-1003

Message `<timestamp>, [CVLC-1003], <sequence-number>,, INFO, <system-name>, Forceful LUN policy change to clear text while re-key session is still active.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the encryption LUN policy was forcefully changed while a re-key session was still active.

Recommended Action No action is required.

Severity INFO

CVLC-1004

Message `<timestamp>, [CVLC-1004], <sequence-number>,, INFO, <system-name>, Forceful encryption LUN removal while re-key session is still active.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the encryption LUN was forcefully removed while a re-key session was still active.

Recommended Action No action is required.

Severity INFO

CVLC-1005

Message `<timestamp>, [CVLC-1005], <sequence-number>,, INFO, <system-name>, There is no LUN's found from the target.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that there are no LUNs found from the target-initiator pair.

Recommended Action No action is required.

Severity INFO

CVLC-1006

Message `<timestamp>, [CVLC-1006], <sequence-number>,, INFO, <system-name>, Duplicate LUN serial number <LUN SN> found.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>.`

Probable Cause Indicates that there is more than one LUN serial number discovered from the same target. Therefore, encryption on this target is disabled.

Recommended Action No action is required.

Severity WARNING

CVLC-1007

Message `<timestamp>, [CVLC-1007], <sequence-number>,, ERROR, <system-name>, Removal of encryption LUN is not allowed when decrypt of existing data is enabled.\nContainer: <Target container name>, Initiator: <Initiator physical >, LUN ID: <LUN ID>.`

Probable Cause Indicates that there has been an attempt to remove the encryption LUN while decryption of existing data is still enabled.

Recommended Action If you want to preserve the user data, use cryptocfg --modLUNpolicy -cleartext to convert to clear text LUN.

Use cryptocfg ---modLUNpolicy -disable_allowdecrypt to disable decryption of existing data. Then try the LUN deletion again.

Severity ERROR

CVLC-1008

Message `<timestamp>, [CVLC-1008], <sequence-number>,, ERROR, <system-name>, LUN discovery failure: <Discovery state>, Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that LUN discovery failed.

Recommended Action No action is required.

Severity ERROR

CVLC-1009

Message `<timestamp>, [CVLC-1009], <sequence-number>,, ERROR, <system-name>, Wrong device type: should be <Expected device type (Disk/Tape)>, found <Discovered device type (Disk/Tape)>.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that LUN discovery failed.

Recommended Action No action is required.

Severity ERROR

CVLC-1010

Message `<timestamp>, [CVLC-1010], <sequence-number>,, ERROR, <system-name>, Tape license is required for tape container: <Target container name>.`

Probable Cause Indicates that the tape container is configured with non-Brocade mode but there is no valid license.

Recommended Action Obtain license for non-Brocade mode.

Severity ERROR

CVLC-1011

Message `<timestamp>, [CVLC-1011], <sequence-number>,, ERROR, <system-name>, Third party license is required for encryption LUN in third party mode.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the encryption LUN is configured with non-Brocade mode but there is no valid license.

Recommended Action Obtain license for non-Brocade mode.

Severity ERROR

CVLC-1012

Message `<timestamp>, [CVLC-1012], <sequence-number>,, ERROR, <system-name>, Disk metadata is in wrong format (<Metadata format found (Brocade/Third party)>).\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the metadata found on the disk LUN is in the wrong format.

Recommended Action Use **cryptocfg** command to change the LUN's metadata mode.

Severity ERROR

CVLC-1013

Message `<timestamp>, [CVLC-1013], <sequence-number>,, ERROR, <system-name>, Unable to retrieve key record from the key archive.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the encryption engine is unable to retrieve the key record base on the key ID found in the metadata.

Recommended Action No action is required.

Severity ERROR

CVLC-1014

Message `<timestamp>, [CVLC-1014], <sequence-number>,, ERROR, <system-name>, Missing Key ID from user input.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the data state in the LUN configuration is in the encrypted state without a key ID and there is no metadata found on the LUN.

Recommended Action Use **cryptocfg** command to add the key ID, if available.

Severity ERROR

CVLC-1015

Message `<timestamp>, [CVLC-1015], <sequence-number>,, ERROR, <system-name>, LUN is set to read only mode. Reason: <Reason for LUN is set to read only mode>.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the LUN is set as read-only because there is a conflict in the configuration.

Recommended Action No action is required.

Severity INFO

CVLC-1016

Message `<timestamp>, [CVLC-1016], <sequence-number>,, INFO, <system-name>, LUN is out of read only mode. Reason: <Reason for LUN is out of read only mode>.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the LUN is set back to read/write.

Recommended Action No action is required.

Severity INFO

CVLC-1017

Message `<timestamp>, [CVLC-1017], <sequence-number>,, INFO, <system-name>, Event: <Description of the event>.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates a warning or an error event.

Recommended Action No action is required.

Severity INFO

CVLC-1018

Message `<timestamp>, [CVLC-1018], <sequence-number>,, INFO, <system-name>, Event: <Description of the event>.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates an informational event.

Recommended Action No action is required.

Severity INFO

CVLC-1019

Message `<timestamp>, [CVLC-1019], <sequence-number>,, ERROR, <system-name>, Metadata exists while data state is clear text.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the data state in the LUN configuration is in clear text state but metadata exists on the LUN.

Recommended Action Use **cryptocfg** command to confirm the configuration.

Severity ERROR

CVLC-1020

Message `<timestamp>, [CVLC-1020], <sequence-number>,, ERROR, <system-name>, Metadata exists while LUN is clear text.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that metadata exists on the LUN that is clear text.

Recommended Action Use **cryptocfg** command to confirm the configuration.

Severity ERROR

CVLC-1021

Message `<timestamp>, [CVLC-1021], <sequence-number>,, INFO, <system-name>, User provided key ID <Key ID from metadata> is ignored while metadata <Key ID provided by the user> exists.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the key ID provided is ignored because metadata exists on the LUN.

Recommended Action No action is required.

Severity INFO

CVLC-1022

Message `<timestamp>, [CVLC-1022], <sequence-number>,, INFO, <system-name>, User provided key ID <Key ID from metadata> is ignored while data state is clear text.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the key ID provided is ignored because the data state is clear text.

Recommended Action No action is required.

Severity INFO

CVLC-1023

Message `<timestamp>, [CVLC-1023], <sequence-number>,, INFO, <system-name>, Rebalance recommended on EE: <EE name>.`

Probable Cause Indicates that due to container configuration changes, weights are not balanced on OB1s.

Recommended Action Run "cryptocfg –rebalance" to increase system performance.

Severity INFO

CVLC-1024

Message `<timestamp>, [CVLC-1024], <sequence-number>,, INFO, <system-name>, Device Decommission operation <Decommission state (succeeded/failed)>.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the device decommission process has either succeeded or failed.

Recommended Action No action is required.

Severity INFO

CVLC-1025

Message `<timestamp>, [CVLC-1025], <sequence-number>,, ERROR, <system-name>, Secondary Metadata exists for encrypted LUN not configured with -newLUN option .\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the secondary metadata exists on the LUN that is not configured with –newLUN option.

Recommended Action Use th ecryptocfg command to remove and add the LUN with –newLUN option.

Severity ERROR

CVLC-1026

Message `<timestamp>, [CVLC-1026], <sequence-number>,, INFO, <system-name>, Some secondary metadata missing for encrypted LUN configured with -newLUN option.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that the secondary metadata does not exist on all LBAs for a LUN that is configured with –newLUN option.

Recommended Action No action is required.

Severity INFO

CVLC-1027

Message `<timestamp>, [CVLC-1027], <sequence-number>,, ERROR, <system-name>, Encrypted LUN configured with -newLUN option does not contain any metadata.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates the metadata was corrupted.

Recommended Action No action is required.

Severity ERROR

CVLC-1028

Message `<timestamp>, [CVLC-1028], <sequence-number>,, WARNING, <system-name>, Not starting auto rekey on LUN with uncompressible blocks 1-16.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates a warning event.

Recommended Action Perform a manual rekey on this LUN.

Severity WARNING

CVLC-1029

Message `<timestamp>, [CVLC-1029], <sequence-number>,, WARNING, <system-name>, Mirror LUN is disabled as primary LUN is being rekeyed without splitting the mirror.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates performing FTE or manual rekey of primary LUN without splitting the mirror.

Recommended Action Break the mirror and re-establish the mirror after rekey on primary LUN is complete.

Severity WARNING

CVLC-1030

Message `<timestamp>, [CVLC-1030], <sequence-number>,, WARNING, <system-name>, Primary LUN may be out of sync with mirror LUN.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates the manual rekey was completed on primary LUN.

Recommended Action

1. Make the target ports of the mirror LUN offline to hosts.
2. Re-establish the mirror.
3. Once the mirror is in sync, split the mirror.
4. Bring back the target ports of the mirror LUN online.

Severity WARNING

CVLC-1031

Message `<timestamp>, [CVLC-1031], <sequence-number>,, WARNING, <system-name>, Primary LUN is restored from mirror LUN. LUN in read-only mode.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates a rekeyed primary LUN may have been restored from mirror LUN without synchronizing.

Recommended Action

1. Create a new primary LUN.
2. Add it to its container with -newLUN option.
3. Using host based migration application, copy data from old to new primary LUN.

Severity WARNING

CVLC-1032

Message `<timestamp>, [CVLC-1032], <sequence-number>,, INFO, <system-name>, Secondary metadata for LUN has been restored.\nContainer: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates the host I/Os to secondary metadata region.

Recommended Action No action is required.

Severity INFO

CVLC-1033

Message `<timestamp>, [CVLC-1033], <sequence-number>,, INFO, <system-name>, Rebalance completed for EE: <EE name>\nDevice login in progress.`

Probable Cause Indicates a rebalance operation was performed.

Recommended Action No action is required.

Severity INFO

CVLC-1034

Message `<timestamp>, [CVLC-1034], <sequence-number>,, INFO, <system-name>, Rekey failed on Container: <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID> because <Failure reason>.`

Probable Cause Indicates the First time encryption, Key expired or Manual re-key operation failed.

Recommended Action No action is required.

Severity INFO

CVLC-1035

Message `<timestamp>, [CVLC-1035], <sequence-number>,, ERROR, <system-name>, A decommissioned LUN has been added back as encrypted LUN. Container <Target container name>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.`

Probable Cause Indicates that decommissioned LUN has been added back as encrypted LUN.

Recommended Action

1. Remove LUN from container.
2. Add it back as a cleartext LUN.
3. Modify LUN policy to encrypt.

Severity ERROR

Chapter

CVLM System Messages

20

CVLM-1001

Message `<timestamp>, [CVLM-1001], <sequence-number>,, ERROR, <system-name>, Failed to allocate memory: <function name>.`

Probable Cause Indicates that the specified function has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **memShow** command. Restart or power cycle the switch.

Severity ERROR

CVLM-1002

Message `<timestamp>, [CVLM-1002], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module> rc = <error>.`

Probable Cause Indicates that an initialization of a module within the CVLMD has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

CVLM-1003

Message `<timestamp>, [CVLM-1003], <sequence-number>,, INFO, <system-name>, Crypto device configuration has been committed by switch <Switch WWN>.`

Probable Cause Indicates that the switch has committed a crypto device configuration.

Recommended Action No action is required.

Severity INFO

CVLM-1004

Message `<timestamp>, [CVLM-1004], <sequence-number>,, WARNING, <system-name>, Crypto device configuration between local switch <local switch WWN> and peer <peer switch WWN> is out of sync. New encryption session is not allowed.`

Probable Cause Indicates that EE nodes in the cluster encryption group have different configurations.

Recommended Action Synchronize the configuration in the cluster group using the **cryptocfg –commit** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity WARNING

CVLM-1005

Message `<timestamp>, [CVLM-1005], <sequence-number>,, INFO, <system-name>, Crypto service is <status> on the switch.`

Probable Cause Indicates that Crypto service is enabled or disabled on the switch.

Recommended Action No action is required.

Severity INFO

CVLM-1006

Message `<timestamp>, [CVLM-1006], <sequence-number>,, WARNING, <system-name>, Crypto device <device WWN> in target container <container name> is not in AD0.`

Probable Cause Indicates that the crypto device in the crypto target container is not in AD0.

Recommended Action Use the **ad** command to move the crypto device into AD0. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity WARNING

CVLM-1007

Message `<timestamp>, [CVLM-1007], <sequence-number>,, WARNING, <system-name>, Redirect zone update failure. Status is <status>.`

Probable Cause Indicates that the redirect zone update has failed.

Recommended Action Issue the **cryptocfg –commit** command again. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity WARNING

CVLM-1008

Message `<timestamp>, [CVLM-1008], <sequence-number>,, WARNING, <system-name>, The member <EE node WWN><EE slot num> of HAC <HAC name> is not in the fabric.`

Probable Cause Indicates that the member of HAC is not in the fabric.

Recommended Action Check the ISL port connected to the fabric.

Severity WARNING

CVLM-1009

Message `<timestamp>, [CVLM-1009], <sequence-number>,, INFO, <system-name>, The member <EE node WWN><EE slot num> of HAC <HAC name> is in the fabric.`

Probable Cause Indicates that the member of HAC is found in the fabric.

Recommended Action No action is required.

Severity INFO

CVLM-1010

Message `<timestamp>, [CVLM-1010], <sequence-number>,, WARNING, <system-name>, The IP address of EE <EE node WWN><EE slot num> IO link is not configured.`

Probable Cause Indicates that the EE IO link IP address is not configured.

Recommended Action Configure the EE IO link IP address.

Severity WARNING

CVLM-1011

Message `<timestamp>, [CVLM-1011], <sequence-number>,, INFO, <system-name>, The HAC failover occurs at EE <EE node WWN><EE slot num>.`

Probable Cause Indicates that the HAC failover occurs at the EE.

Recommended Action No action is required.

Severity INFO

CVLM-1012

Message `<timestamp>, [CVLM-1012], <sequence-number>,, INFO, <system-name>, The HAC failback occurs at EE <EE node WWN><EE slot num>.`

Probable Cause Indicates that the HAC failback occurs at the EE.

Recommended Action No action is required.

Severity INFO

CVLM-3001

Message `<timestamp>, [CVLM-3001], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Failback mode set to <failbackmode>.`

Probable Cause Indicates the failback mode was set.

Recommended Action No action is required.

Severity INFO

CVLM-3002

Message `<timestamp>, [CVLM-3002], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: HA cluster <HAClusterName> created.`

Probable Cause Indicates an HA cluster was created.

Recommended Action No action is required.

Severity INFO

CVLM-3003

Message `<timestamp>, [CVLM-3003], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: HA cluster <HAClusterName> deleted.`

Probable Cause Indicates an HA cluster was deleted.

Recommended Action No action is required.

Severity INFO

CVLM-3004

Message `<timestamp>, [CVLM-3004], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Cluster member added to HA cluster <HAClusterName>.`

Probable Cause Indicates an HA cluster member was added to an HA cluster.

Recommended Action No action is required.

Severity INFO

CVLM-3005

Message `<timestamp>, [CVLM-3005], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Cluster member removed from HA cluster <HAClusterName>.`

Probable Cause Indicates an HA cluster member was removed from an HA cluster.

Recommended Action No action is required.

Severity INFO

CVLM-3006

Message `<timestamp>, [CVLM-3006], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Current node WWN/slot <CurrentWWN> / <CurrentSlot> replaced with new node WWN/slot: <NewWWN> / <NewSlot>.`

Probable Cause Indicates an HA cluster member was replaced.

Recommended Action No action is required.

Severity INFO

CVLM-3007

Message `<timestamp>, [CVLM-3007], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: <diskOrTape> container \<containerName>\ created.`

Probable Cause Indicates a cryptotarget container was created.

Recommended Action No action is required.

Severity INFO

CVLM-3008

Message `<timestamp>, [CVLM-3008],<sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Container \<containerName>\ deleted.`

Probable Cause Indicates a cryptotarget container was deleted.

Recommended Action No action is required.

Severity INFO

CVLM-3009

Message
```
<timestamp>, [CVLM-3009], <sequence-number>,, INFO, <system-name>, Event:
cryptocfg Status: success, Info: Manual failback from EE
<currentnodeWWN>/<currentSlot> to EE <newnodeWWN>/<newnodeSlot>.
```

Probable Cause Indicates a manual failback was performed to an encryption engine.

Recommended Action No action is required.

Severity INFO

CVLM-3010

Message
```
<timestamp>, [CVLM-3010],<sequence-number>,, INFO, <system-name>, Event:
cryptocfg Status: success, Info: Move crypto container \<cryptoTargetContainer>\
to EE <newEEWWN>/<newEESlot>.
```

Probable Cause Indicates a cryptotarget container was moved to another encryption engine.

Recommended Action No action is required.

Severity INFO

CVLM-3011

Message
```
<timestamp>, [CVLM-3011], <sequence-number>,, INFO, <system-name>, Event:
cryptocfg Status: success, Info: Initiator PWWN \<initiatorPWWN>\ Initiator NWWN
\<initiatorNWWN>\ added to crypto target container \<cryptoTargetContainer>\.
```

Probable Cause Indicates an initiator was added to a cryptotarget container.

Recommended Action No action is required.

Severity INFO

CVLM-3012

Message
```
<timestamp>, [CVLM-3012],<sequence-number>,, INFO, <system-name>, Event:
cryptocfg Status: success, Info: Initiator \<initiator>\ removed from crypto
target container \<cryptoTargetContainer>\.
```

Probable Cause Indicates an initiator was removed from a cryptotarget container.

Recommended Action No action is required.

Severity INFO

CVLM-3013

Message
```
<timestamp>, [CVLM-3013], <sequence-number>,, INFO, <system-name>, Event:
cryptocfg Status: success, Info: LUN <LUNSpec>, attached through Initiator
\<Initiator>\, added to crypto target container \<cryptoTargetContainer>\.
```

Probable Cause Indicates a LUN was added to a cryptotarget container.

Recommended Action No action is required.

Severity INFO

CVLM-3014

Message
```
<timestamp>, [CVLM-3014], <sequence-number>,, INFO, <system-name>, Event:
cryptocfg Status: success, Info: Lun <LUNNumber>, attached through Initiator
\<Initiator>\, in crypto target container \<cryptoTargetContainer>\ modified.
```

Probable Cause Indicates a LUN in a cryptotarget container was modified.

Recommended Action No action is required.

Severity INFO

CVLM-3015

Message
```
<timestamp>, [CVLM-3015], <sequence-number>,, INFO, <system-name>, Event:
cryptocfg Status: success, Info: Lun <LUNNumber>, attached through Initiator
\<Initiator>\, removed from crypto target container \<cryptoTargetContainer>\.
```

Probable Cause Indicates a LUN was removed from a cryptotarget container.

Recommended Action No action is required.

Severity INFO

CVLM-3016

Message `<timestamp>, [CVLM-3016], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Lun <LUNNumber>, attached through Initiator \<Initiator>\, in crypto target container \<cryptoTargetContainer>\ enabled.`

Probable Cause Indicates a LUN in a cryptotarget container was enabled.

Recommended Action No action is required.

Severity INFO

CVLM-3017

Message `<timestamp>, [CVLM-3017], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Tape pool \<tapepoolLabelOrNum>\ created.`

Probable Cause Indicates a tapepool was created.

Recommended Action No action is required.

Severity INFO

CVLM-3018

Message `<timestamp>, [CVLM-3018], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Tape pool \<tapepoolLabelOrNum>\ deleted.`

Probable Cause Indicates a tapepool was deleted.

Recommended Action No action is required.

Severity INFO

CVLM-3019

Message `<timestamp>, [CVLM-3019], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Tape pool \<tapepoolLabelOrNum>\ modified.`

Probable Cause Indicates a tapepool was modified.

Recommended Action No action is required.

Severity INFO

CVLM-3020

Message `<timestamp>, [CVLM-3020], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Manual rekey of LUN <LUNSpec> attached through Initiator \<Initiator>\ in crypto tgt container \<cryptoTargetContainer>\.`

Probable Cause Indicates a manual rekey of a LUN was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3021

Message `<timestamp>, [CVLM-3021], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Manual rekey all performed.`

Probable Cause Indicates a complete manual rekey was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3022

Message `<timestamp>, [CVLM-3022], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Resume rekey of LUN <LIUNSpec> attached through Initiator \<Initiator>\ in crypto tgt container \<cryptoTargetContainer>\.`

Probable Cause Indicates a resume rekey was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3023

Message `<timestamp>, [CVLM-3023], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Transaction committed.`

Probable Cause Indicates a transaction commit operation was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3024

Message `<timestamp>, [CVLM-3024], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Transaction <transactionID> aborted.`

Probable Cause Indicates a transaction abort operation was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3025

Message `<timestamp>, [CVLM-3025], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: started, Info: Decommission of device (container <cryptoTargetContainer> initiator <Initiator>, LUN <Lun>).`

Probable Cause Indicates that the decommission operation has started.

Recommended Action No action is required.

Severity INFO

CVLM-3026

Message `<timestamp>, [CVLM-3026], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: failed, Info: Decommission of device (container <cryptoTargetContainer> initiator <Initiator>, LUN <Lun>).`

Probable Cause Indicates that the decommission operation has failed for the device.

Recommended Action Reissue the decommission command.

Severity INFO

CVLM-3027

Message `<timestamp>, [CVLM-3027], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Decommission of device (container <cryptoTargetContainer> initiator <Initiator>, LUN <Lun>).`

Probable Cause Indicates that the decommission operation has been completed for the device.

Recommended Action No action is required.

Severity INFO

CVLM-3028

Message `<timestamp>, [CVLM-3028], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: SRDF mode set to <srdfmode>.`

Probable Cause Indicates that the SRDF mode was set.

Recommended Action No action is required.

Severity INFO

Chapter

DAUTH System Messages

21

DOT1-1001

Message `<timestamp>, [DOT1-1001], <sequence-number>,, INFO, 802.1X is enabled globally.`

Probable Cause Indicates that the 802.1X is enabled globally.

Recommended Action No action is required.

Severity INFO

DOT1-1002

Message `<timestamp>, [DOT1-1002], <sequence-number>,, INFO, 802.1X is disabled globally.`

Probable Cause Indicates that the 802.1X is disabled globally.

Recommended Action No action is required.

Severity INFO

DOT1-1003

Message `<timestamp>, [DOT1-1003], <sequence-number>,, INFO, 802.1X is enabled for port <port_name>.`

Probable Cause Indicates that the 802.1X is enabled for a particular port.

Recommended Action No action is required.

Severity INFO

DOT1-1004

Message `<timestamp>, [DOT1-1004], <sequence-number>,, INFO, Port <port_name> is forcefully unauthorized.`

Probable Cause Indicates that the port is unauthorized forcefully.

Recommended Action No action is required.

Severity INFO

DOT1-1005

Message `<timestamp>, [DOT1-1005], <sequence-number>,, INFO, 802.1X Authentication is successful on port <port_name>.`

Probable Cause Indicates that the authentication has succeeded on a particular port.

Recommended Action No action is required.

Severity INFO

DOT1-1006

Message `<timestamp>, [DOT1-1006], <sequence-number>,, WARNING, 802.1X Authentication has failed on port <port_name>.`

Probable Cause Indicates that the authentication has failed on a particular port.

Recommended Action Check the credentials configured with Supplicant and the RADIUS server.

Severity WARNING

DOT1-1007

Message `<timestamp>, [DOT1-1007], <sequence-number>,, CRITICAL, No RADIUS server available for authentication.`

Probable Cause Indicates that there are no RADIUS servers available for authentication.

Recommended Action Check whether the configured RADIUS servers are reachable and are functioning.

Severity CRITICAL

DOT1-1008

Message `<timestamp>, [DOT1-1008], <sequence-number>,, INFO, Port <port_name> is forcefully authorized.`

Probable Cause Indicates that the port is authorized forcefully.

Recommended Action No action is required.

Severity INFO

DOT1-1009

Message `<timestamp>, [DOT1-1009], <sequence-number>,, INFO, 802.1X is disabled for port <port_name>.`

Probable Cause Indicates that the 802.1X is disabled for a particular port.

Recommended Action No action is required.

Severity INFO

DOT1-1010

Message `<timestamp>, [DOT1-1010], <sequence-number>,, INFO, Port <port_name> is set in auto mode.`

Probable Cause Indicates that the port is set to auto mode.

Recommended Action No action is required.

Severity INFO

Chapter

EM System Messages

22

EM-1001

Message `<timestamp>, [EM-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, <FRU ID> is over heating: Shutting down.`

Probable Cause Indicates that a field-replaceable unit (FRU) is shutting down due to overheating. This is typically due to a faulty fan but can also be caused by the switch environment.

Recommended Action Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Run the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at a high enough speed, they should be replaced.

Severity CRITICAL

EM-1002

Message `<timestamp>, [EM-1002], <sequence-number>, FFDC, INFO, <system-name>, System fans status <fan FRU>.`

Probable Cause Indicates that a nonbladed system has overheated and may shut down. All fan speeds are dumped to the console.

Recommended Action Verify that the location temperature is within the operational range of the switch. Refer to the *Hardware Reference Manual* for the environmental temperature range of your switch.

Run the **fanShow** command to verify that all fans are running at normal speeds. If any fans are missing or are not performing at a high enough speed, they should be replaced.

Severity INFO

EM-1003

Message `<timestamp>, [EM-1003], <sequence-number>, FFDC, CRITICAL, <system-name>, <FRU ID> has unknown hardware identifier: FRU faulted.`

Probable Cause Indicates that a field-replaceable unit (FRU) header could not be read or is not valid. The FRU is faulted.

Recommended Action On Brocade 24000 and 48000, try reseating the specified FRU.

Restart or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. To run this command root access is required. Refer to the *Fabric OS Command Reference* for more information on this command.

On the Brocade 24000 and 48000, replace the specified FRU.

For the Brocade 3900, replace the motherboard FRU.

For the Brocade 200E, 3016, 3250, 3850, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, and AP7600, replace the switch.

Severity CRITICAL

EM-1004

Message `<timestamp>, [EM-1004], <sequence-number>, FFDC, CRITICAL, <system-name>, <FRU ID> failed to power on.`

Probable Cause Indicates that a field-replaceable unit (FRU) failed to power on and is not being used. The type of FRU is specified in the message.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port.

The Brocade 3250 has one power supply and three fans, and the Brocade 3850 has two power supplies and four fans. Values for the individual fans and power supplies for these switches might display, but these parts cannot be replaced: the entire switch is a FRU.

The Brocade 3016 does not have any fans, power supplies or world wide name (WWN) cards.

The Brocade 200E, 4012, 4016, 4018, 4020, and 4024 have 4 fans and 1 power supply, but these parts cannot be replaced: the entire switch is a FRU.

Recommended Action Try reseating the FRU. If the message persists, replace the FRU.

Severity CRITICAL

EM-1005

Message `<timestamp>, [EM-1005], <sequence-number>, FFDC, CRITICAL, <system-name>, <FRU Id> has faulted. Sensors above maximum limits.`

Probable Cause Indicates that a blade in the specified slot or the switch (for nonbladed switches) is being shut down for environmental reasons; its temperature or voltage is out of range.

Recommended Action Check the environment and make sure the room temperature is within the operational range of the switch. Use the **fanShow** command to verify fans are operating properly. Make sure there are no blockages of the airflow around the chassis. If the temperature problem is isolated to the blade itself, replace the blade.

Voltage problems on a blade are likely a hardware problem on the blade itself; replace the blade.

Severity CRITICAL

EM-1006

Message `<timestamp>, [EM-1006], <sequence-number>, FFDC, CRITICAL, <system-name>, <FRU Id> has faulted. Sensors below minimum limits.`

Probable Cause Indicates that the sensors show the voltage is below minimum limits. The switch or specified blade is being shut down for environmental reasons; the voltage is too low.

Recommended Action If this problem occurs on a blade, it usually indicates a hardware problem on the blade; replace the blade.

If this problem occurs on a switch, it usually indicates a hardware problem on the main board; replace the switch.

Severity CRITICAL

EM-1007

Message `<timestamp>, [EM-1007], <sequence-number>, FFDC, CRITICAL, <system-name>, <FRU Id> is being reset. Sensors has exceeded max limits.`

Probable Cause Indicates that the voltage on a switch has exceeded environmental limits. A reset is sent to the faulty slot or the switch for nonbladed switches.

Recommended Action There is most likely a voltage hardware problem on the blade or motherboard of the switch.

For the Brocade DCX, 24000 and 48000, replace the blade field-replaceable unit (FRU).

For the Brocade 3900 replace the motherboard FRU.

For the Brocade 200E, 3016, 3250, 3850, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, AP7600, replace the switch.

Severity CRITICAL

EM-1008

Message `<timestamp>, [EM-1008], <sequence-number>, FFDC, CRITICAL, <system-name>, Unit in <Slot number or Switch> with ID <FRU Id> is faulted, it is incompatible with the <type of incompatibility> configuration.`

Probable Cause Indicates that a blade inserted in the specified slot or the switch (for nonbladed switches) is not compatible with either the platform configuration or the logical switch configuration. The blade is faulted.

Recommended Action If the blade is not compatible, replace the blade and ensure the replacement blade is compatible with your control processor (CP) type. If the incompatibility is with the logical switch configuration, change the configuration with the **lscfg** command to be consistent with the blade type or remove the blade.

Severity CRITICAL

EM-1009

Message `<timestamp>, [EM-1009], <sequence-number>, FFDC, CRITICAL, <system-name>, <FRU Id> powered down unexpectedly.`

Probable Cause Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). This might indicate a hardware malfunction in the FRU.

Recommended Action Try reseating the FRU. If the message persists, replace the FRU. Refer to the *Brocade 48000 Hardware Reference Manual* for more information about **chassisConfig** modes and supported blades.

Severity CRITICAL

EM-1010

Message `<timestamp>, [EM-1010], <sequence-number>, FFDC, CRITICAL, <system-name>, Received unexpected power down for <FRU Id> But <FRU Id> still has power.`

Probable Cause Indicates that the environmental monitor (EM) received an unexpected power-down notification from the specified field-replaceable unit (FRU). However, the specified FRU still appears to be powered up after four seconds.

Recommended Action Try reseating the blade. If this fails to correct the error, replace the blade.

Severity CRITICAL

EM-1011

Message `<timestamp>, [EM-1011], <sequence-number>, FFDC, CRITICAL, <system-name>, Received unexpected power down for <FRU Id>, but cannot determine if it has power.`

Probable Cause Indicates that the environmental monitor (EM) received an unexpected power-down notification from the field-replaceable unit (FRU) specified; however, after four seconds it cannot be determined if it has powered down or not.

Recommended Action Try reseating the blade. If this fails to correct the error, replace the blade.

Severity CRITICAL

EM-1012

Message `<timestamp>, [EM-1012], <sequence-number>, FFDC, CRITICAL, <system-name>, <FRU Id> failed <state> state transition, unit faulted.`

Probable Cause Indicates that a switch blade or nonbladed switch failed to transition from one state to another. It is faulted. The specific failed target state is displayed in the message. There are serious internal Fabric OS configuration or hardware problems on the switch.

Recommended Action On Brocade DCX, 24000 and 48000, try reseating the indicated field-replaceable unit (FRU). If the message persists, restart or power cycle the switch. Run the **systemVerification** command to verify that the switch does not have hardware problems. To run this command root access is required. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

If the message persists, replace the FRU.

Severity CRITICAL

EM-1013

Message `<timestamp>, [EM-1013], <sequence-number>,, ERROR, <system-name>, Failed to update FRU information for <FRU Id>.`

Probable Cause Indicates that the environmental monitor (EM) was unable to update the time alive or the original equipment manufacturer (OEM) data in the memory on a field-replaceable unit (FRU).

Recommended Action If you ran the **fruInfoSet** command, try the command again; otherwise, the update is automatically attempted again. If it continues to fail, try reseating the FRU.

If the message persists, replace the FRU.

Severity ERROR

EM-1014

Message `<timestamp>, [EM-1014], <sequence-number>,, ERROR, <system-name>, Unable to read sensor on <FRU Id> (<Return code>)`

Probable Cause Indicates that the environmental monitor was unable to access the sensors on the specified field-replaceable unit (FRU).

Recommended Action Try reseating the FRU. If the message persists, replace the FRU.

Severity ERROR

EM-1015

Message `<timestamp>, [EM-1015], <sequence-number>,, WARNING, <system-name>, Warm recovery failed (<Return code>).`

Probable Cause Indicates that a problem was discovered when performing consistency checks during a warm boot.

Recommended Action Monitor the switch. If the problem persists, a **reBoot** or power cycle is required to resolve the problem.

Severity WARNING

EM-1016

Message `<timestamp>, [EM-1016], <sequence-number>,, WARNING, <system-name>, Cold recovery failed (<Return code>).`

Probable Cause Indicates that a problem was discovered when performing consistency checks during a cold boot.

Recommended Action Monitor the switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

EM-1017

Message `<timestamp>, [EM-1017], <sequence-number>,, WARNING, <system-name>, Uncommitted WWN change detected. Cold reboot required.`

Probable Cause Indicates that a user did not commit a changed world wide name (WWN) value prior to executing a **reboot**, **power cycle**, or **firmwareDownload** operation.

Recommended Action Change and commit the new WWN value.

Severity WARNING

EM-1018

Message `<timestamp>, [EM-1018], <sequence-number>, FFDC, CRITICAL, <system-name>, CP blade in slot <slot number> failed to retrieve current chassis type (<detailed fault descriptor>/<PLACE HOLDER>/0x<PLACE HOLDER>).`

Probable Cause Indicates that there was a failure to read the chassis type from the system.

Recommended Action Verify that the control processor (CP) blade is operational and is properly seated in its slot.

Severity CRITICAL

EM-1019

Message `<timestamp>, [EM-1019], <sequence-number>,, WARNING, <system-name>, Current chassis configuration option (<Chassis config option currently in effect>) is not compatible with standby firmware version (Pre 4.4), cannot allow HA Sync.`

Probable Cause Indicates that the current **chassisConfig** option is not supported by the firmware on the standby control processor (CP). This is true even if the standby comes up and appears to be operational. High availability (HA) synchronization of the CPs will not be allowed.

Recommended Action Either change the **chassisConfig** option to 1 with the **chassisConfig** command, or upgrade the firmware on the standby to the version running on the active CP.

Severity WARNING

EM-1028

Message

```
<timestamp>, [EM-1028], <sequence-number>, FFDC, WARNING, <system-name>, HIL
Error: <function> failed to access history log for FRU: <FRU Id> (rc=<return
code>).
```

Probable Cause Indicates a problem accessing the data on the world wide name (WWN) card field-replaceable unit (FRU) or the WWN card storage area on the main logic board.

The problems were encountered when the software attempted to write to the history log storage to record an event for the specified FRU. The return code is for internal use only. This can indicate a significant hardware problem.

The *FRU ID* value is composed of a FRU type string and an optional number to identify the unit, slot, or port.

Recommended Action If the message persists, reboot or power cycle the switch.

If the message still persists, replace the WWN card, or the switch (for nonbladed switches).

Severity WARNING

EM-1029

Message

```
<timestamp>, [EM-1029], <sequence-number>,, WARNING, <system-name>, <FRU Id>, a
problem occurred accessing a device on the I2C bus (<error code>). Operational
status (<state of the FRU when the error occurred>) not changed, access is being
retried.
```

Probable Cause Indicates that the I2C bus had problems and a timeout occurred.

Recommended Action This is often a transient error.

Watch for the EM-1048 message, which indicates that the problem has been resolved.

If the error persists, check for loose or dirty connections. Remove all dust and debris prior to reseating the field-replaceable unit (FRU). If it continues to fail, replace the FRU.

Severity WARNING

EM-1031

Message

```
<timestamp>, [EM-1031], <sequence-number>,, ERROR, <system-name>, <FRU Id>
ejector not closed.
```

Probable Cause Indicates that the environmental monitor (EM) has found a switch blade that is inserted, but the ejector switch is not closed. The blade in the specified slot is treated as not inserted.

Recommended Action Close the ejector switch (raise the slider in most blades, or completely screw in the upper thumbscrew for the FC4-48 port blade) if the field-replaceable unit (FRU) is intended for use. Refer to the appropriate hardware manual for instructions on inserting the switch blades.

Severity ERROR

EM-1033

Message `<timestamp>, [EM-1033], <sequence-number>,, ERROR, <system-name>, CP in <FRU Id> set to faulty because CP ERROR asserted`

Probable Cause Indicates that the standby control processor (CP) has been detected as faulty. The High Availability (HA) feature will not be available. This message occurs every time the other CP reboots, even as part of a clean warm failover. In most situations, this message is followed by the EM-1047 message, and no action is required for the CP; however, you might want to find out why the failover occurred.

Recommended Action If the standby CP was just rebooted, wait for the error to clear (run **slotShow** to determine if it has cleared). Watch for the EM-1047 message to verify that this error has cleared.

If the standby CP continues to be faulty or if it was not intentionally rebooted, check the error logs on the other CP (using the **errDump** command) to determine the cause of the error state.

Try reseating the field-replaceable unit (FRU). If the message persists, replace the FRU.

Severity ERROR

EM-1034

Message `<timestamp>, [EM-1034], <sequence-number>,, ERROR, <system-name>, <FRU Id> set to faulty, rc=<return code>.`

Probable Cause Indicates that the specified field-replaceable unit (FRU) has been marked as faulty for the specified reason.

Recommended Action Try reseating the FRU.

Run the **systemVerification** command to verify that the switch does not have hardware problems. To run this command root access is required. Refer to the *Fabric OS Command Reference* for more information on this command.

If the message persists, replace the FRU.

Severity ERROR

EM-1035

Message <timestamp>, [EM-1035], <sequence-number>,, ERROR, <system-name>, 2 circuit paired Power Supplies are faulty, please check the <Switch side> AC main switch/circuit to see if it has power.

Probable Cause Suggests that since both power supplies associated with one of the two main circuits are present but faulty, maybe the circuit's switch has been turned off, or the AC power source has been interrupted for that circuit.

The *Switch side* value is either "left" or "right" designating which circuit switch, facing the cable side of the chassis. The Switch side value indicates:

- left: controls the odd numbered power supply units.
- right: controls the even numbered power supply units.

Recommended Action Check that the identified AC circuit switch is turned on, that the power cord is properly attached and undamaged, and that the power source is operating properly.

Severity ERROR

EM-1036

Message `<timestamp>, [EM-1036], <sequence-number>,, WARNING, <system-name>, <FRU Id> is not accessible.`

Probable Cause Indicates that the specified field-replaceable unit (FRU) does not seem to be present on the switch.

If the FRU is a world wide name (WWN) card, then default WWN and IP addresses are used for the switch.

Recommended Action Reseat the FRU card.

If the message persists, reboot or power cycle the switch.

Run the **systemVerification** command to verify that the switch does not have hardware problems. To run this command root access is required. Refer to the *Fabric OS Command Reference* for more information on this command.

If the message persists, replace the FRU.

Severity WARNING

EM-1037

Message `<timestamp>, [EM-1037], <sequence-number>,, INFO, <system-name>, <FRU Id> is no longer faulted.`

Probable Cause Indicates that the specified power supply has been marked as no longer being faulty, probably because its AC power supply has been turned on.

Recommended Action No action is required.

Severity INFO

EM-1041

Message `<timestamp>, [EM-1041], <sequence-number>,, WARNING, <system-name>, Sensor values for <FRU Id>: <Sensor Value> <Sensor Value> <Sensor Value> <Sensor Value> <Sensor Value> <Sensor Value> <Sensor Value>.`

Probable Cause Indicates that sensors detected a warning condition. All significant sensors for the field-replaceable unit (FRU) are displayed; each contains a header.

This message can display:

- voltages in volts
- temperature in Celsius
- fan speeds in RPM

Recommended Action If the message is isolated, monitor the error messages on the switch. If the message is associated with other messages, follow the recommended action for those messages.

Severity WARNING

EM-1042

Message `<timestamp>, [EM-1042], <sequence-number>,, WARNING, <system-name>, Important FRU header data for <FRU Id> is not valid).`

Probable Cause Indicates that the specified field-replaceable unit (FRU) has an incorrect number of sensors in its FRU header-derived information. This could mean that the FRU header was corrupted or read incorrectly or corrupted in the object database, which contains information about all FRUs.

Recommended Action Try reseating the FRU. If the message persists, replace the FRU.

Severity WARNING

EM-1043

Message `<timestamp>, [EM-1043], <sequence-number>,, WARNING, <system-name>, Can't power <FRU Id> <state (on or off)>.`

Probable Cause Indicates that the specified field-replaceable unit (FRU) cannot be powered on or off.

Recommended Action The specified FRU is not responding to commands and should be replaced.

Severity WARNING

EM-1044

Message `<timestamp>, [EM-1044], <sequence-number>,, WARNING, <system-name>, Can't power on <FRU Id>, its logical switch is shut down`

Probable Cause Indicates that the specified field-replaceable unit (FRU) cannot be powered on because the associated logical switch is shut down.

Recommended Action Run the **switchStart** command on the associated logical switch.

Severity WARNING

EM-1045

Message `<timestamp>, [EM-1045], <sequence-number>,, WARNING, <system-name>, <FRU Id> is being powered <new state>.`

Probable Cause Indicates that an automatic power adjustment is being made because of the (predicted) failure of a power supply or the insertion or removal of a port blade. If new_state is On, a port blade is being powered on because more power is available (either a power supply was inserted or a port blade was removed or powered down). If new_state is Off, a port blade has been powered down because a power supply has been faulted, because it is indicating a predicted failure. If new_state is Down (not enough power), a newly inserted port blade was not powered on because there was not enough power available.

Recommended Action The Brocade 24000 requires only a single power supply for a fully populated chassis; however, you should always operate the system with at least two power supplies for redundancy.

Severity WARNING

EM-1046

Message `<timestamp>, [EM-1046], <sequence-number>,, WARNING, <system-name>, Sysctrl reports error status for blade ID <id value> for the blade in slot <slot number> <blade incompatibility type: platform, backplane, or switch configuration>`

Probable Cause Indicates that the blade specified is incompatible.

Recommended Action If the blade ID listed is not correct, then the field-replaceable unit (FRU) header for the blade is corrupted and the blade must be replaced. If the reason is due to platform, the blade ID listed is not supported for that platform (CP) type. Remove the blade from the chassis. If the reason is due to backplane, the CP type (CP256) is not supported on that chassis (backplane revision D2), remove the blade from the chassis.

If the reason is switch configuration, the blade's logical switch configuration is not correct. Run the **lscfg** command to correct the switch or port configuration for the ports on that blade.

Severity WARNING

EM-1047

Message `<timestamp>, [EM-1047], <sequence-number>,, INFO, <system-name>, CP in slot <slot number> not faulty, CP ERROR deasserted.`

Probable Cause Indicates that the control processor (CP) is no longer faulted. This message usually follows EM-1033. The new standby CP is in the process of rebooting and has turned off the CP_ERR signal.

Recommended Action No action is required.

Severity INFO

EM-1048

Message `<timestamp>, [EM-1048], <sequence-number>,, INFO, <system-name>, <FRU Id> I2C access recovered: state <current state>`

Probable Cause Indicates that the I2C bus problems have been resolved and I2C access to the field-replaceable unit (FRU) has become available again.

Recommended Action The EM-1029 error can be a transitory error; if the problem resolves, the EM-1048 message is displayed.

Severity INFO

EM-1049

Message `<timestamp>, [EM-1049], <sequence-number>,, INFO, <system-name>, FRU <FRU Id> insertion detected.`

Probable Cause Indicates that a field-replaceable unit (FRU) of the type and location specified by the FRU ID was detected as having been inserted into the chassis.

Recommended Action No action is required.

Severity INFO

EM-1050

Message `<timestamp>, [EM-1050], <sequence-number>,, INFO, <system-name>, FRU <FRU Id> removal detected.`

Probable Cause Indicates that a field-replaceable unit (FRU) of the specified type and location was removed from the chassis.

Recommended Action Verify that the FRU was intended to be removed. Replace the FRU as soon as possible.

Severity INFO

EM-1051

Message `<timestamp>, [EM-1051], <sequence-number>,, INFO, <system-name>, <FRU Id>: Inconsistency detected, FRU re-initialized.`

Probable Cause Indicates that an inconsistent state was found in the field-replaceable unit (FRU). This occurs if the state of the FRU was changing during a failover. The FRU is reinitialized and traffic might have been disrupted.

Recommended Action No action is required.

Severity INFO

EM-1057

Message `<timestamp>, [EM-1057], <sequence-number>,, WARNING, <system-name>, Blade:<Slot Id> is getting reset:<Fault reason>.`

Probable Cause Indicates the blade is being automatically reset because of known resetable transient errors such as an application-specific integrated circuit (ASIC) parity error.

Recommended Action No action is required if the switch does not reach the reset threshold for the switch or blade. If the reset threshold is reached on the switch or blade, the switch or blade will be faulted and should be replaced.

Severity WARNING

EM-1058

Message `<timestamp>, [EM-1058], <sequence-number>,, WARNING, <system-name>, Switch gets reset:<Fault reason>`

Probable Cause Indicates the switch is being automatically reset because of a known resetable transient problem such as an application-specific integrated circuit (ASIC) parity error.

Recommended Action No action is required if the switch does not reach the reset threshold for the switch or blade. If the reset threshold is reached on the switch or blade, the switch or blade will be faulted and should be replaced.

Severity WARNING

EM-1059

Message `<timestamp>, [EM-1059], <sequence-number>, FFDC, ERROR, <system-name>, <Slot number or Switch> with id <FRU Id> cannot be found in the fru description xml file.`

Probable Cause Indicates that a blade inserted in the specified slot or the switch (for nonbladed switches) is not compatible with the switch configuration software. The system may not be usable.

Recommended Action Replace the blade. Make sure the replacement is compatible with your switch type.

Severity ERROR

EM-1060

Message `<timestamp>, [EM-1060], <sequence-number>,, WARNING, <system-name>, Stopping synchronization of the system due to blade incompatibility with software version on standby CP.`

Probable Cause Indicates a blade in the system is not supported by the release on the standby control processor (CP).

Recommended Action Remove all blades of this type or upgrade your standby CP. Once an appropriate action is taken, this CP must be rebooted or the **haSyncStart** command must be run successfully. Until this is done, the system will remain out of synchronization.

Severity WARNING

EM-1061

Message `<timestamp>, [EM-1061], <sequence-number>,, WARNING, <system-name>, Synchronization halted. Remove all blades of type <Blade Type Id> or upgrade your standby CP, then reboot or run haSyncStart.`

Probable Cause Indicates a blade in the system is not supported by the release on the standby control processor (CP).

Recommended Action Remove all blades of this type or upgrade your standby CP. Once an appropriate action is taken, this CP must be rebooted or the **haSyncStart** command must be run successfully. Until this is done, the system will remain out of synchronization.

Severity WARNING

EM-1062

Message `<timestamp>, [EM-1062], <sequence-number>,, CRITICAL, <system-name>, Blade in slot <Slot Id> faulted as it exceeds the maximum support limit of <Limit> blades with Blade ID <Blade Type Id> in the chassis.`

Probable Cause Indicates too many blades of a particular type are in the system.

Recommended Action Remove the faulted blade.

Severity CRITICAL

EM-1063

Message `<timestamp>, [EM-1063], <sequence-number>,, CRITICAL, <system-name>, Blade in slot <Slot Id> faulted because it exceeds the maximum support limit of <Limit> blades with Blade IDs <Applicable blade Type IDs> in the chassis.`

Probable Cause Indicates too many blades of a set of particular types are in the system.

Recommended Action Remove the faulted blade.

Severity CRITICAL

EM-1064

Message `<timestamp>, [EM-1064], <sequence-number>,, CRITICAL, <system-name>, Blade:<slot ID> is being powered off (based on user configuration) upon receiving a HW ASIC ERROR, reason:<Fault reason>.`

Probable Cause Indicates the blade is being powered off because a hardware (HW) application specific integrated circuit (ASIC) ERROR was detected, and you have selected to power off the problem blade when such a condition occurred.

Recommended Action Contact the switch provider for support.

Severity CRITICAL

EM-1065

Message `<timestamp>, [EM-1065], <sequence-number>,, WARNING, <system-name>, SSAS Virtualization Services are not available due to incompatibility between the FOS and SAS versions<Slot number or blank for single board systems>.`

Probable Cause Indicates the version of either the control processor firmware (CFOS) or the blade processor firmware (BFOS) is not compatible with the Storage Application Services (SAS) or other application firmware versions.

Recommended Action Upgrade the FOS firmware or the SAS firmware with the **firmwareDownload** command. Refer to the release notes for a compatible version of firmware.

Severity WARNING

EM-1066

Message `<timestamp>, [EM-1066], <sequence-number>,, INFO, <system-name>, SAS Virtualization Services are now available <Slot number or blank for single board systems>.`

Probable Cause Indicates the previously incompatible Fabric OS or Storage Application Services (SAS) firmware has been upgraded and is now compatible.

Recommended Action No action is required.

Severity INFO

EM-1067

Message `<timestamp>, [EM-1067], <sequence-number>,, WARNING, <system-name>, Stopping synchronization of the system due to version incompatibility with standby CP.`

Probable Cause Indicates that the software version on the standby CP is not compatible with this software version.

Recommended Action Upgrade the software on the standby CP or downgrade the software on this CP.

Severity WARNING

EM-1068

Message `<timestamp>, [EM-1068], <sequence-number>,, ERROR, <system-name>, High Availability Service Management subsystem failed to respond.  A required component is not operating.`

Probable Cause Indicates that the HA subsystem has not returned a response within four minutes of the request from the Environmental Manager. It usually indicates that some component has not started properly or has terminated. The specific component that has failed might be indicated in other messages or debug data. There are serious internal Fabric OS configuration or hardware problems on the switch.

Recommended Action Reboot or power cycle the switch. If the message persists, collect switch information using the **supportsave** command, and contact your switch service provider.

Severity ERROR

EM-1069

Message `<timestamp>, [EM-1069], <sequence-number>,, INFO, <system-name>, Slot <FRU slot number> is being powered off.`

Probable Cause Indicates a blade is being intentionally powered off.

Recommended Action No action is required.

Severity INFO

EM-1070

Message `<timestamp>, [EM-1070], <sequence-number>,, INFO, <system-name>, Slot <FRU slot number> is being powered on.`

Probable Cause Indicates a blade is being intentionally powered on.

Recommended Action No action is required.

Severity INFO

EM-2003

Message `<timestamp>, [EM-2003], <sequence-number>,, ERROR, <system-name>, <Slot Id or Switch for pizza boxes> has failed the POST tests. FRU is being faulted.`

Probable Cause Indicates that a field-replaceable unit (FRU) has failed the Power-On Self-Test. Refer to the */tmp/post[1/2].slot#.log* file for more information on faults. To view this log file you must be logged in at the root level. The ID will be Switch for non-bladed systems.

Recommended Action On bladed systems, try reseating the specified FRU.

On nonbladed switches, reboot or power cycle the switch.

If the problem persists:

- Run the **systemverification** command to verify that the switch does not have hardware problems. To run this command root access is required. Refer to the*Fabric OS Reference Manual* for more information on this command.
- On bladed systems, replace the specified FRU; otherwise replace the switch.

Severity ERROR

Chapter

ESS System Messages

23

ESS-1001

Message `<timestamp>, [ESS-1001], <sequence-number>,, WARNING, <system-name>, A few switches in the fabric do not support the Coordinated HotCode protocol.`

Probable Cause Indicates one or more switches in the fabric do not support the Coordinated HotCode protocol. Continuing with the firmware download may cause data traffic disruption.

Recommended Action Discontinue the firmware download, identify the downlevel switch or switches that do not support the Coordinated HotCode protocol, and upgrade the downlevel switches. Then, restart the firmware download on this switch. Note that upgrading a downlevel Brocade switch in a mixed interop fabric may still cause data traffic disruption.

Severity WARNING

ESS-1002

Message `<timestamp>, [ESS-1002], <sequence-number>,, WARNING, <system-name>, The pause message is rejected by the domain <domain id>.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected pause message.

Recommended Action No action is required.

Severity WARNING

ESS-1003

Message `<timestamp>, [ESS-1003], <sequence-number>,, WARNING, <system-name>, The pause retry count is exhausted for the domain <domain id>.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action No action is required.

Severity WARNING

ESS-1004

Message `<timestamp>, [ESS-1004], <sequence-number>,, WARNING, <system-name>, The resume message is rejected by the domain <domain id>.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected resume message.

Recommended Action No action is required.

Severity WARNING

ESS-1005

Message `<timestamp>, [ESS-1005], <sequence-number>,, WARNING, <system-name>, The resume retry count is exhausted for the domain <domain id>.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action No action is required.

Severity WARNING

Chapter

ESWCH System Messages

24

ESW-1001

Message `<timestamp>, [ESW-1001], <sequence-number>,, ERROR, <system-name>, Switch is not in ready state - Switch enable failed switch status= 0x<switch status>, c_flags = 0x<switch control flags>.`

Probable Cause Indicates that the switch enable has failed.

Recommended Action If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

ESW-1002

Message `<timestamp>, [ESW-1002], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized device <wwn name of device> tries to flogin to port <port number>.`

Probable Cause Indicates that the device is not present in the authorized profile list.

Recommended Action Verify that the device is authorized to log in to the switch. If the device is authorized, first run the **secPolicyDump** command to verify whether the specified device world wide name (WWN) is listed. If it is not listed, run the **secPolicyAdd** command to add this device to an existing policy.

Severity INFO

ESW-1003

Message `<timestamp>, [ESW-1003], <sequence-number>,, ERROR, <system-name>, Slot ENABLED but Not Ready during recovery, disabling slot = <slot number>(<return value>).`

Probable Cause Indicates that the slot state has been detected as inconsistent during failover or recovery.

Recommended Action On a Brocade 8000 switch, restart or power cycle the switch.

Severity ERROR

ESW-1004

Message `<timestamp>, [ESW-1004], <sequence-number>,, ERROR, <system-name>,Blade attach failed during recovery, disabling slot = <slot number>.`

Probable Cause Indicates that the blade has failed during failover or recovery.

Recommended Action On a Brocade 8000 switch, restart or power cycle the switch.

Severity ERROR

ESW-1005

Message `<timestamp>, [ESW-1005], <sequence-number>,, ERROR, <system-name>,Diag attach failed during recovery, disabling slot = <slot number>.`

Probable Cause Indicates that the **Diag blade attach** command has failed during failover or recovery.

Recommended Action On a Brocade 8000 switch, restart or power cycle the switch.

Severity ERROR

ESW-1006

Message `<timestamp>, [ESW-1006], <sequence-number>,, WARNING, <system-name>, HA state out of sync: Standby CP (ver = <standby SWC version>) does not support NPIV functionality. (active ver = <active SWC version>, NPIV devices = <'1' if NPIV devices exist; Otherwise '0'>).`

Probable Cause Indicates that the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) functionality, but the switch has some NPIV devices logged into the fabric.

Recommended Action Load a firmware version on standby that supports NPIV functionality, using the **firmwareDOwnload** command.

Severity WARNING

ESW-1007

Message `<timestamp>, [ESW-1007], <sequence-number>,, WARNING, <system-name>,Switch port <port number> disabled due to \"<disable reason>\".`

Probable Cause Indicates that the switch port is disabled due to the reason displayed in the message.

Recommended Action Based on the disable reason displayed, take appropriate action to restore the port. Insufficient frame buffers: Reduce the distance or speed settings for the port to reduce the buffer requirement of the link. Alternatively, one or more ports in the port group must be disabled to make more buffers available for the link. Refer to the *Fabric OS Administrator's Guide* for more information.

Severity WARNING

ESW-1008

Message `<timestamp>, [ESW-1008], <sequence-number>,, WARNING, <system-name>,<area string> are port swapped on ports that do not support port swap. Slot <slot number> will be faulted.`

Probable Cause Indicates that the blade has area swapped ports on ports that do not support this feature.

Recommended Action Replace the blade with ports that support port swap. Refer to the *Fabric OS Administrator's Guide* for more information.

Severity WARNING

Chapter

EVMD System Messages

25

EVMD-1001

Message `<timestamp>, [EVMD-1001], <sequence-number>,, WARNING, <system-name>, Event could not be sent to remote proxy. = <Remote proxy switch id.>`

Probable Cause Indicates the event could not be sent to remote proxy. This could happen if the remote proxy switch cannot be reached through in-band.

The event could not be sent to the remote proxy because the remote proxy switch cannot be reached through in-band.

Recommended Action Please make sure that the specified remote domain is present in the fabric.

Severity WARNING

Chapter

FABR System Messages

26

FABR-1001

Message `<timestamp>, [FABR-1001], <sequence-number>,, WARNING, <system-name>, port <port number>, <segmentation reason>.`

Probable Cause Indicates that the specified switch port is isolated because of a segmentation resulting from mismatched configuration parameters.

Recommended Action Based on the segmentation reason displayed within the message, look for a possible mismatch of relevant configuration parameters in the switches at both ends of the link.

Run the **configure** command to modify the appropriate switch parameters on both the local and remote switch.

Severity WARNING

FABR-1002

Message `<timestamp>, [FABR-1002], <sequence-number>,, WARNING, <system-name>, fabGaid: no free multicast alias IDs.`

Probable Cause Indicates that the fabric does not have any available multicast alias IDs to assign to the alias server.

Recommended Action Verify alias IDs using the **fabricShow** command on the principal switch.

Severity WARNING

FABR-1003

Message `<timestamp>, [FABR-1003], <sequence-number>,, WARNING, <system-name>, port <port number>: ILS <command> bad size <payload size>, wanted <expected payload size>.`

Probable Cause Indicates that an internal link service (ILS) information unit of invalid size has been received. The neighbor switch has sent a payload with an invalid size.

Recommended Action Investigate the neighbor switch for problems. Run the **errShow** command on the neighbor switch to view the error log for additional messages.

Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or SFP if necessary.

Run the **portLogDumpPort** command on both the receiving and transmitting ports.

Run the **fabStateShow** command on both the receiving and transmitting switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1004

Message `<timestamp>, [FABR-1004], <sequence-number>,, WARNING, <system-name>, port: <port number>, req iu: 0x<address of IU request sent>, state: 0x<command sent>, resp iu: 0x<address of response IU received>, state 0x<response IU state>, <additional description>.`

Probable Cause Indicates that the information unit response was invalid for the specified command sent. The fabric received an unknown response. This message is rare and usually indicates a problem with the Fabric OS kernel.

Recommended Action If this message is due to a one-time event because of the incoming data, the system will discard the frame. If it is due to problems with the kernel, the system will recover by performing a failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1005

Message `<timestamp>, [FABR-1005], <sequence-number>,, WARNING, <system-name>, <command sent>: port <port number>: status 0x<reason for failure> (<description of failure reason>) xid = 0x<exchange ID of command>.`

Probable Cause Indicates that the application failed to send an async command for the specified port. The message provides additional details regarding the reason for the failure and the exchange ID of the command. This can happen if a port is about to go down.

Recommended Action No action is required. This message is often transitory.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1006

Message `<timestamp>, [FABR-1006], <sequence-number>,, WARNING, <system-name>, Node free error, caller: <error description>.`

Probable Cause Indicates that the Fabric OS is trying to free or deallocate memory space that has already been deallocated. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action In case of severe memory corruption, the system might recover by performing an automatic failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1007

Message `<timestamp>, [FABR-1007], <sequence-number>,, WARNING, <system-name>, IU free error, caller: <function attempting to de-allocate IU>.`

Probable Cause Indicates that a failure occurred when deallocating an information unit. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action In case of severe memory corruption, the system might recover by performing an automatic failover.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1008

Message `<timestamp>, [FABR-1008], <sequence-number>,, WARNING, <system-name>, <error description>.`

Probable Cause Indicates that errors occurred during the request domain ID state; the information unit (IU) cannot be allocated or sent. If this message occurs with FABR-1005, the problem is usually transitory. Otherwise, this message is rare and usually indicates a problem with the Fabric OS. The error descriptions are as follows:

- FAB RDI: cannot allocate IU
- FAB RDI: cannot send IU

Recommended Action No action is required if the message appears with the FABR_1005 message.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1009

Message `<timestamp>, [FABR-1009], <sequence-number>,, WARNING, <system-name>, <error description>.`

Probable Cause Indicates that errors were reported during the exchange fabric parameter state; cannot allocate domain list due to a faulty exchange fabric parameter (EFP) type. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action The fabric daemon will discard the EFP. The system will recover through the EFP retrial process.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1010

Message `<timestamp>, [FABR-1010], <sequence-number>,, WARNING, <system-name>, <error description>.`

Probable Cause Indicates that the errors occurred while cleaning up the request domain ID (RDI). The error description provides further details. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1011

Message `<timestamp>, [FABR-1011], <sequence-number>, FFDC, ERROR, <system-name>, <error description>.`

Probable Cause Indicates that the Fabric OS is unable to inform the Fabric OS State Synchronization Management module (FSSME) that the fabric is stable or unstable. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

FABR-1012

Message `<timestamp>, [FABR-1012], <sequence-number>,, WARNING, <system-name>, <function stream>: no such type, <invalid type>.`

Probable Cause Indicates that the fabric is not in the appropriate state for the specified process. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action The fabric daemon will take proper action to recover from the error.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FABR-1013

Message `<timestamp>, [FABR-1013], <sequence-number>, FFDC, CRITICAL, <system-name>, No Memory: pid=<fabric process id> file=<source file name> line=<line number within the source file>.`

Probable Cause Indicates that there is not enough memory in the switch for the fabric module to allocate. This message is rare and usually indicates a problem with the Fabric OS.

Recommended Action The system will recover by failing over to the standby CP.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

FABR-1014

Message `<timestamp>, [FABR-1014], <sequence-number>, FFDC, ERROR, <system-name>, Port <port number> Disabled: Insistent Domain ID <Domain ID> could not be obtained. Principal Assigned Domain ID = <Domain ID>`

Probable Cause Indicates that the specified port received an request domain ID (RDI) accept message containing a principal-switch-assigned domain ID that is different from the insistent domain ID (IDID). Fibre connectivity (FICON) mode requires an insistent domain ID. If an RDI response has a different domain ID, then the port is disabled.

Recommended Action Run the **configShow** command to view the fabric.ididmode. A '0' means the IDID mode is disabled; a '1' means it is enabled.

Set the switch to insistent domain ID mode. This mode is set under the **configure** command or in Web Tools on the **Switch Admin > Configure** window.

Severity ERROR

FABR-1015

Message `<timestamp>, [FABR-1015], <sequence-number>, FFDC, ERROR, <system-name>, FICON Insistent DID max retry exceeded: All E-Ports will be disabled. Switch is isolated.`

Probable Cause Indicates that the application exceeded request domain ID (RDI) requests for the insistent domain ID. All E_Ports are disabled, isolating the specified switch from the fabric.

Recommended Action Verify that the insistent domain ID is unique in the fabric and then re-enable the E_Ports. Run the **fabricShow** command to view the domain IDs across the fabric and the **configure** command to change the insistent domain ID mode. Refer to the *Fabric OS Command Reference* for more information on these commands.

Severity ERROR

FABR-1016

Message `<timestamp>, [FABR-1016], <sequence-number>,, WARNING, <system-name>, ficonMode is enabled.`

Probable Cause Indicates that FICON mode is enabled on the switch through a user interface command.

Recommended Action No action is required.

Severity WARNING

FABR-1017

Message `<timestamp>, [FABR-1017], <sequence-number>,, WARNING, <system-name>, ficonMode is disabled.`

Probable Cause Indicates that FICON mode is disabled on the switch through a user interface command.

Recommended Action No action is required.

Severity WARNING

FABR-1018

Message `<timestamp>, [FABR-1018], <sequence-number>,, WARNING, <system-name>, PSS principal failed (<reason for not becoming the principal switch>: <WWN of new principal switch>).`

Probable Cause Indicates that a failure occurred when trying to set the principal switch using the **fabricPrincipal** command. The message notifies you that the switch failed to become the principal switch because of one of the following reasons:

- The switch joined an existing fabric and bypassed the F0 state.
- The fabric already contains a principal switch that has a lower world wide name (WWN).

Recommended Action Make sure that no other switch is configured as the principal switch. Force a fabric rebuild by using the **switchDisable** and **switchEnable** commands.

Refer to the *Fabric OS Command Reference* for more information about the **fabricPrincipal** command.

Severity WARNING

FABR-1019

Message `<timestamp>, [FABR-1019], <sequence-number>, FFDC, CRITICAL, <system-name>, Critical fabric size (<current domains>) exceeds supported configuration (<supported domains>).`

Probable Cause Indicates that this switch is a value-line switch and has exceeded the limited fabric size: that is, a specified limit to the number of domains. This limit is defined by your specific value-line license key. The fabric size has exceeded this specified limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity CRITICAL

FABR-1020

Message `<timestamp>, [FABR-1020], <sequence-number>, FFDC, CRITICAL, <system-name>, Web Tools will be disabled in <days> days <hours> hours and <minutes> minutes.`

Probable Cause Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This message displays the number of days left in the grace period. After this time, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity CRITICAL

FABR-1021

Message `<timestamp>, [FABR-1021], <sequence-number>, FFDC, CRITICAL, <system-name>, Web Tools is disabled.`

Probable Cause Indicates that this switch has a value-line license and has a limited number of domains. If more than the specified number of domains are in the fabric, a counter is started to disable Web Tools. This grace period has expired and Web Tools has been disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity CRITICAL

FABR-1022

Message `<timestamp>, [FABR-1022], <sequence-number>, FFDC, CRITICAL, <system-name>, Fabric size (<actual domains>) exceeds supported configuration (<supported domains>). Fabric limit timer (<type>) started from <grace period in seconds>.`

Probable Cause Indicates that the fabric size has exceeded the value-line limit, and the grace period counter has started. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity CRITICAL

FABR-1023

Message `<timestamp>, [FABR-1023], <sequence-number>,, INFO, <system-name>, Fabric size is within supported configuration (<supporteddomains>). Fabric limit timer (<type>) stopped at <grace period in seconds>.`

Probable Cause Indicates that the fabric size is within specified limits. Either a full fabric license was added or the size of the fabric was changed to within the licensed limit.

Recommended Action No action is required.

Severity INFO

FABR-1024

Message `<timestamp>, [FABR-1024], <sequence-number>,, INFO, <system-name>, Initializing fabric size limit timer <grace period>`

Probable Cause Indicates that the fabric size has exceeded the limit set by your value-line switches. Value-line switches have a limited fabric size, i.e., a specified limit to the number of domains. This value is defined by your specific value-line license key. The fabric size has exceeded this specified limit. The grace-period timer has been initialized. If the grace period is complete and the size of the fabric is still outside the specified limit, Web Tools is disabled.

Recommended Action Bring the fabric size within the licensed limits. Either a full fabric license must be added or the size of the fabric must be changed to within the licensed limit. Contact your switch provider to obtain a full fabric license.

Severity INFO

FABR-1029

Message `<timestamp>, [FABR-1029], <sequence-number>,, INFO, <system-name>, Port <port number> negotiated <flow control mode description> (mode = <received flow control mode>).`

Probable Cause Indicates that a different flow control mode, as described in the message, is negotiated with the port at the other end of the link. The flow control is a mechanism of throttling the transmitter port to avoid buffer overrun at the receiving port. There are three types of flow control modes:

- VC_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.
- R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.
- DUAL_CR mode: Dual-credit flow control mode. In both of the previous modes, the buffer credits are fixed, based on the port configuration information. In this mode, the buffer credits are negotiated as part of exchange link parameter (ELP) exchange. This mode also uses the R_RDY primitive for flow control.

Recommended Action No action is required.

Severity INFO

FABR-1030

Message `<timestamp>, [FABR-1030], <sequence-number>,, INFO, <system-name>, fabric: Domain <new domain ID> (was <old domain ID>).`

Probable Cause Indicates that the domain ID has changed.

Recommended Action No action is required.

Severity INFO

FABR-1031

Message `<timestamp>, [FABR-1031], <sequence-number>, FFDC, WARNING, <system-name>, Maximum number of retries sending ILS from port <port number> exceeded.`

Probable Cause Indicates the fabric exhausted the maximum number of retries sending internal link service (ILS) to the iswitchd demon on the specified E_Port.

Recommended Action Run the **top** command to see if iswitchd is extremely busy or if another process is using excessive CPU resources.

Severity WARNING

FABR-1032

Message `<timestamp>, [FABR-1032], <sequence-number>, WARNING, <system-name>, Remote switch with domain ID <domain ID>and switchname <switchname>running an unsupported FOS version v2.x has joined the fabric.`

Probable Cause Indicates that a switch with an unsupported Fabric OS version 2.x has joined the fabric.

Recommended Action Remove the switch with the unsupported Fabric OS version 2.x from the fabric.

Severity WARNING

FABR-1034

Message `<timestamp>, [FABR-1034], <sequence-number>, INFO, <system-name>, Area <Area that has already been acquired> have been acquired by port <Port that has already acquired the area>. Persistently disabling port <Port that is being disabled>.`

Probable Cause Indicates you must enable Trunk Area on a port for another port to use the same area.

Recommended Action Move the cable to a port area that is not in use, or disable Trunk Area. You must manually enable the port or the port remains disabled forever.

Refer to the *Fabric OS Administrator's Guide* for more information.

Severity INFO

FABR-1035

Message `<timestamp>, [FABR-1035], <sequence-number>, INFO, <system-name>, Slave area <Area that does not match Master port's area> does not match Master port <Master port>. Persistently disabling port <Port that is being disabled>.`

Probable Cause Indicates the Slave port's Trunk Area differs from that of the Master port.

Recommended Action Move the cable to a port to match with the same Master Trunk Area, or disable Trunk Area. You must manually enable the port or the port remains disabled forever.

Refer to the *Admin Guide* for more information.

Severity INFO

FABR-1036

Message `<timestamp>, [FABR-1036], <sequence-number>, INFO, <system-name>, F_port trunks are only allowed on Trunk Area enabled port. Persistently disabling port <Port that is being disabled>.`

Probable Cause Indicates the specified port is being disabled because when the port on a Switch is Trunk Area enabled, it does not allow other devices like AG or HBA that are not Trunk Area enabled.

Recommended Action Move the cable to a port that does not have Trunk Area enabled.

Severity INFO

FABR-1037

Message `<timestamp>, [FABR-1037], <sequence-number>, INFO, <system-name>, Port configuration incompatible with Trunk Area enabled port. Persistently disabling port <Port that is being disabled>.`

Probable Cause Indicates the specified port is being disabled because when the port attempts to go online, the Switch finds that Trunk Area enabled is incompatible with port configuration such as long distance, port mirror, fast write or EX_port.

Recommended Action Check the port configuration to disable long distance, port mirror, fast write or EX_port.

Severity INFO

FABR-1038

Message `<timestamp>, [FABR-1038], <sequence-number>, INFO, <system-name>, Trunking license not present with F_port trunking enabled. Persistently disabling port <Port that is being disabled>.`

Probable Cause Indicates the specified port is being disabled because F_port trunking is enabled without a trunking license being present.

Recommended Action Install a trunking license or disable F_port trunking on the port.

Severity INFO

FABR-1039

Message `<timestamp>, [FABR-1039], <sequence-number>, WARNING, <system-name>, Invalid domain id zero received from principal switch (domain id=<Principal domain id>).`

Probable Cause Indicates an invalid domain ID zero has been received.

Recommended Action Check the principal switch for the invalid domain ID zero.

Severity WARNING

FABR-1040

Message `<timestamp>, [FABR-1040], <sequence-number>, INFO, <system-name>, Speed is not 2g,4g or 8g with F_port trunking enabled. Persistently disabling port <Port that is being disabled>.`

Probable Cause Indicates that the speed is not compatible for F_port trunks.

Recommended Action Change the speed for the port or disable F_port trunking on the port.

Severity INFO

FABR-1041

Message `<timestamp>, [FABR-1041], <sequence-number>, ERROR, <system-name>, Port <Port that is being disabled> is disabled due to trunk protocol error.`

Probable Cause Indicates a link reset was received before the completion of the trunking protocol on the port.

Recommended Action Enable the port by running the **portEnable** command. The port may recover by re-initialization of the link. If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers followed by the **supportSave** command and contact your switch service provider.

Severity ERROR

FABR-1043

Message `<timestamp>, [FABR-1043], <sequence-number>, ERROR, <system-name>, Detected Fabric ID conflict with remote (not neighbor) switch <Switchname> (domain <Domain ID>), FID <Fabric ID>. No local E-ports disabled.`

Probable Cause Indicates that the remote switch has a Fabric ID conflict with the local switch. But no ports are disabled because the remote switch is not adjacent to the local switch.

Recommended Action Make sure that all the switches in the fabric have the same Fabric ID or upgrade the switch firmware to a VF-capable firmware.

Severity ERROR

FABR-1044

Message `<timestamp>, [FABR-1044], <sequence-number>, ERROR, <system-name>, Detected Fabric ID conflict with neighbor switch <Switchname> (domain <Domain ID>), FID <Fabric ID>. E-ports (<Number of E-ports disabled>) connected to the switch are disabled.`

Probable Cause Indicates that the neighbor switch has a Fabric ID conflict with the local switch. All E_ports directly connected to the conflicting switch are disabled.

Recommended Action Make sure that all the switches in the fabric have the same fabric ID or upgrade the switch firmware to a VF-capable firmware.

Severity ERROR

FABR-1045

Message `<timestamp>, [FABR-1045], <sequence-number>, ERROR, <system-name>, <Text>Detected Base Switch conflict with remote (not neighbor) switch <Switchname> (domain <Domain ID>), BS <Base Switch Mode>. No local E-ports disabled.`

Probable Cause Indicates that the remote switch has a Base Switch attribute conflict with the local switch. But no ports are disabled because the remote switch is not adjacent to the local switch.

Recommended Action Make sure that all the switches in the fabric have the same Base Switch attribute or disable VF mode for the conflicting switch using the **fosconfig** command.

Severity ERROR

FABR-1046

Message `<timestamp>, [FABR-1046], <sequence-number>, ERROR, <system-name>, Detected Base Switch conflict with neighbor switch <Switchname> (domain <Domain ID>), BS <Base Switch Mode>. E-ports (<Number of E-ports disabled>) connected to the switch are disabled.`

Probable Cause Indicates that the remote switch has a Base Switch attribute conflict with the local switch. All the E_ports directly connected to the conflicting switch are disabled.

Recommended Action Make sure that all the switches in the fabric have the same Base Switch attribute or upgrade the switch firmware to a VF-capable firmware.

Severity ERROR

FABR-1047

Message `<timestamp>, [FABR-1047], <sequence-number>, INFO, <system-name>, Area unavailable to assign to the port. Persistently disabling port <Port that is being disabled>.`

Probable Cause Indicates that there are no areas available to assign to the port during port creation.

Recommended Action Move some ports out of the default switch to make areas available.

Severity INFO

FABR-1048

Message `<timestamp>, [FABR-1048], <sequence-number>, ERROR, <system-name>, Detected Fabric ID (FID <InheritedFID> inherited) conflict with remote (not neighbor) switch <Switchname> (domain <Domain ID>, FID <Fabric ID>). No local E-ports disabled.`

Probable Cause Indicates that the remote switch has a Fabric ID conflict with the inherited FID of the local switch. But no ports are disabled because the remote switch is not adjacent to the local switch.

Recommended Action Make sure that all the switches in the fabric have same Fabric ID or upgrade the switch firmware to a VF-capable firmware.

Severity ERROR

FABR-1049

Message `<timestamp>, [FABR-1049], <sequence-number>, ERROR, <system-name>, Detected Fabric ID (FID <InheritedFID> inherited) conflict with neighbor switch <Switchname> (domain <Domain ID>, FID <Fabric ID>). E-ports (<Number of E-ports disabled>) connected to the switch are disabled.`

Probable Cause Indicates that the neighbor switch has Fabric ID conflict with the inherited FID of the local switch. All E_ports directly connected to the conflicting switch are disabled.

Recommended Action Make sure that all the switches in the fabric have same Fabric ID or upgrade the switch firmware to a VF-capable firmware.

Severity ERROR

Chapter

FABS System Messages

27

FABS-1001

Message `<timestamp>, [FABS-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, <Function name> <Description of memory need>`

Probable Cause Indicates that the system is low on memory and cannot allocate more memory for new operations. This is usually an internal Fabric OS problem or file corruption. *Description of memory need* indicates how much memory was being requested. The value could be any whole number.

Recommended Action Reboot or power cycle the switch.

Severity CRITICAL

FABS-1002

Message `<timestamp>, [FABS-1002], <sequence-number>,, WARNING, <system-name>, <Function name> <Description of problem>`

Probable Cause Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

FABS-1004

Message `<timestamp>, [FABS-1004], <sequence-number>,, WARNING, <system-name>, <Function name and description of problem> process <Process ID number> (<Current command name>) <Pending signal number>`

Probable Cause Indicates that an operation has been interrupted by a signal. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

Severity WARNING

FABS-1005

Message `<timestamp>, [FABS-1005], <sequence-number>,, WARNING, <system-name>, <Function name and description of problem> (<ID type>= <ID number>)`

Probable Cause Indicates that an unsupported operation has been requested. This is usually an internal Fabric OS problem or file corruption. The possible value for *function name and description of problem* is:

`fabsys_write: Unsupported write operation: process xxx`

where xxx is the process ID (PID), which could be any whole number.

Recommended Action Reboot or power cycle the active CP (for modular systems) or the switch (for single-board systems).

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

FABS-1006

Message `<timestamp>, [FABS-1006], <sequence-number>,, WARNING, <system-name>, <Function name and description of problem>: object <object type id> unit <slot>`

Probable Cause Indicates that there is no device in the slot with the specified object type ID in the system module record. This could indicate a serious Fabric OS data problem on the switch. The possible values for *function name and description of problem* are:

- setSoftState: bad object
- setSoftState: invalid type or unit
- media_sync: Media oid mapping failed
- fabsys_media_i2c_op: Media oid mapping failed
- fabsys_media_i2c_op: obj is not media type
- media_class_hndlr: failed sending media state to blade driver

Recommended Action If the message is isolated, monitor the error messages on the switch. If the error is repetitive or if the fabric failed, fail over or reboot the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

FABS-1007

Message `<timestamp>, [FABS-1007], <sequence-number>,, WARNING, <system-name>, <Function name>: Media state is invalid - status=<Status value>`

Probable Cause Indicates that the Fabric OS has detected an invalid value in an object's status field. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

FABS-1008

Message `<timestamp>, [FABS-1008], <sequence-number>,, WARNING, <system-name>, <Function name>: Media oid mapping failed`

Probable Cause Indicates that the Fabric OS was unable to locate a necessary object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

Severity WARNING

FABS-1009

Message `<timestamp>, [FABS-1009], <sequence-number>,, WARNING, <system-name>, <Function name>: type is not media`

Probable Cause Indicates that the Fabric OS was unable to locate an appropriate object handle. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

Severity WARNING

FABS-1010

Message `<timestamp>, [FABS-1010], <sequence-number>,, WARNING, <system-name>, <Function name>: Wrong media_event <Event number>`

Probable Cause Indicates that the Fabric OS detected an unknown event type. This is usually an internal Fabric OS problem or file corruption.

Recommended Action Reboot or power cycle the switch.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

FABS-1011

Message `<timestamp>, [FABS-1011], <sequence-number>,, ERROR, <system-name>, <Method name>[<Method tag number>]:Invalid input state 0x<Input state code>`

Probable Cause Indicates an unrecognized state code was used in an internal Fabric OS message for a FRU.

Recommended Action Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity ERROR

FABS-1012

Message

```
<timestamp>, [FABS-1012], <sequence-number>,, ERROR, <system-name>, <Method
name>[<Method tag number>]:FRU state transition failed. Current state 0x<Current
state of FRU> Requested state 0x<Requested new state of FRU> err 0x<Error code>
```

Probable Cause A FRU could not be transitioned to the requested state. This is usually an internal Fabric OS problem.

Recommended Action Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity ERROR

FABS-1013

Message

```
<timestamp>, [FABS-1013], <sequence-number>,, ERROR, <system-name>, <Method
name>[<Method tag number>]:Unknown blade type 0x<Blade type>
```

Probable Cause Indicates an unrecognized type of blade has been discovered in the system.

This may be caused by an incorrect FRU header, inability to read the FRU header, or the blade may not be supported by this platform or Fabric OS version.

Recommended Action Verify that the blade is valid for use in this system and this version of Fabric OS.

Try reseating the blade.

If this is a valid blade and reseating does not fix the problem, then replace the blade.

Severity ERROR

FABS-1014

Message

```
<timestamp>, [FABS-1014], <sequence-number>,, ERROR, <system-name>, <Method
name>[<Method tag number>]:Unknown FRU type 0x<FRU Object type>
```

Probable Cause Indicates an unrecognized type of FRU has been discovered in the system.

This may be caused by an incorrect FRU header, inability to read the FRU header, or the FRU may not be supported by this platform or Fabric OS version.

Recommended Action Verify that the FRU is valid for use in this system and this version of Fabric OS.

Try reseating the FRU.

If this is a valid FRU and reseating does not help, then replace the FRU.

Severity ERROR

FABS-1015

Message `<timestamp>, [FABS-1015], <sequence-number>,, ERROR, <system-name>, <Method name>[<Method tag number>]:Request to enable FRU type 0x<FRU Object type>, unit <Unit number> failed. err code <Error code>`

Probable Cause Indicates the specified FRU could not be enabled. This is usually an internal Fabric OS problem.

Recommended Action Try removing and reinserting the FRU.

Reboot or power-cycle the CP or system.

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity ERROR

Chapter

FBC System Messages

28

FBC-1001

Message `<timestamp>, [FBC-1001], <sequence-number>,, ERROR, <system-name>, Firmware version on AP blade is incompatible with that on the CP.`

Probable Cause The CP determined that the version of firmware running on the AP blade is not compatible with the version of firmware running on the CP. The AP and CP blades cannot communicate.

Recommended Action The problem can be corrected by changing the version of firmware on the CP or AP blades. The firmware version on the CP blade can be changed using the **firmwareDownload** command. Refer to the release notes to determine whether a non-disruptive **firmwareDownload** is supported between the versions. As the AP and CP blades cannot communicate, it is not possible to load new firmware on the AP blade. If required, send the AP blade back to the factory to get a new firmware version installed.

Severity ERROR

Chapter

FCMC System Messages

29

FCMC-1001

Message `<timestamp>, [FCMC-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, System is low on memory and has failed to allocate new memory.`

Probable Cause Indicates that the switch is low on memory and failed to allocate new memory for an information unit (IU).

Recommended Action A nonbladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

Severity CRITICAL

Chapter

FCIP System Messages

30

FCIP-1000

Message `<timestamp>, [FCIP-1000], <sequence-number>, FFDC, ERROR, <system-name>, <command name> of GE <port number> failed. Please retry the command. Data: inst=<ASIC instance> st=<ASIC initializing state> rsn=<reason code> fn=<message function> oid=<ASIC ID>`

Probable Cause Indicates that the hardware is not responding to a command request, possibly because it is busy.

Recommended Action Retry the command.

Severity ERROR

FCIP-1001

Message `<timestamp>, [FCIP-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, FIPS <FIPS Test Name> failed; algo=<algorithm code> type=<algorithm type> slot=<Slot Number>.`

Probable Cause Indicates that an FIPS failure has occured and requires faulting the blade or switch.

Recommended Action Retry the command.

Severity CRITICAL

FCIP-1002

Message `<timestamp>, [FCIP-1002], <sequence-number>, INFO, CFG, <system-name>, An IPsec/IKE policy was added.`

Probable Cause Indicates that an IPsec/IKE policy was added and the config file was updated.

Recommended Action No action is required.

Severity INFO

FCIP-1003

Message `<timestamp>, [FCIP-1003], <sequence-number>, INFO, CFG, <system-name>, An IPsec/IKE policy was deleted.`

Probable Cause Indicates that an IPsec/IKE policy was deleted and the config file was updated.

Recommended Action No action is required.

Severity INFO

FCIP-1004

Message `<timestamp>, [FCIP-1004], <sequence-number>, INFO, CFG, <system-name>, Tape Read Pipelining is being disabled slot (<slot number>) port (<user port index>) tunnel (<The configured tunnel ID (0-7)>).`

Probable Cause Indicates that the FOS version on the remote end of the tunnel does not support Tape Read Pipelining.

Recommended Action No action is required.

Severity INFO

Chapter

FCOE System Messages

31

FCOE-1001

Message `<timestamp>, [FCOE-1001], <sequence-number>,, ERROR, <system-name>, calloc failed for <object>.`

Probable Cause Indicates a memory failure.

Recommended Action Check the switch memory status.

Severity ERROR

FCOE-1002

Message `<timestamp>, [FCOE-1002], <sequence-number>,, WARNING, <system-name>, Max login Group limit reached at <limit>.`

Probable Cause Indicates too many login groups (LGs) have been added.

Recommended Action Check the maximum login group value.

Severity WARNING

FCOE-1003

Message `<timestamp>, [FCOE-1003], <sequence-number>,, INFO, <system-name>, <device>: member in another lg <lg> being removed.`

Probable Cause Indicates that a device is added to some other login group.

Recommended Action Check the login group changes using the **fcoelogincfg –show** command.

Severity INFO

FCOE-1004

Message `<timestamp>, [FCOE-1004], <sequence-number>,, ERROR, <system-name>, <device>: removing member from <lg> failed`

Probable Cause Indicates that the login group has failed.

Recommended Action Remove the failed member from the login group.

Severity ERROR

FCOE-1005

Message `<timestamp>, [FCOE-1005], <sequence-number>,, ERROR, <system-name>, <device>: membership check failed in lg: <lg>`

Probable Cause Indicates that the Membership check for the device has failed.

Recommended Action Check the device for failed Membership.

Severity ERROR

FCOE-1006

Message `<timestamp>, [FCOE-1006], <sequence-number>,, ERROR, <system-name>, file operation failed on <filename> for <operation> operation: errno:<error>.`

Probable Cause Indicates a file operation failure.

Recommended Action Check the error code for file operation failure.

Severity ERROR

FCOE-1007

Message `<timestamp>, [FCOE-1007], <sequence-number>,, ERROR, <system-name>, IfIndex Limit Reached <num_fcoe_entity>.`

Probable Cause Indicates that the IfIndex Limit has reached the maximum.

Recommended Action Check the IfIndex Limit.

Severity ERROR

FCOE-1008

Message `<timestamp>, [FCOE-1008], <sequence-number>,, INFO, <system-name>, Free RASLOG fill this later.`

Probable Cause Indicates an informational message.

Recommended Action No action is required.

Severity INFO

FCOE-1009

Message `<timestamp>, [FCOE-1009], <sequence-number>,, INFO, <system-name>, Addition of nport mapping failed. Max nport mapping limit reached: <maxnport>.`

Probable Cause Indicates that the N_port mapping has reached its maximum limit.

Recommended Action Remove unwanted N_port mappings and try adding N_port mapping.

Severity INFO

FCOE-1010

Message `<timestamp>, [FCOE-1010], <sequence-number>,, ERROR, <system-name>, Cleanup of login failed for port:<port>.`

Probable Cause Indicates an invalid port number.

Recommended Action Use the **supportsave** command and restart the system.

Severity ERROR

FCOE-1011

Message `<timestamp>, [FCOE-1011], <sequence-number>,, ERROR, <system-name>, Request to add errda to VLAN <vid> failed.`

Probable Cause Indicates an add request to a VLAN has failed.

Recommended Action Rerequest to add errda to VLAN.

Severity ERROR

FCOE-1012

Message `<timestamp>, [FCOE-1012], <sequence-number>,, ERROR, <system-name>, Request to delete port from VLAN <vid> failed.`

Probable Cause Indicates a delete port request to a VLAN has failed.

Recommended Action Rerequest to delete port from VLAN.

Severity ERROR

FCOE-1013

Message `<timestamp>, [FCOE-1013], <sequence-number>,, ERROR, <system-name>, Request to add VLAN <vid> failed.`

Probable Cause Indicates an add request to a VLAN has failed.

Recommended Action Rerequest to add VLAN.

Severity ERROR

FCOE-1014

Message `<timestamp>, [FCOE-1014], <sequence-number>,, ERROR, <system-name>, Request to add ports to VLAN <vid> failed.`

Probable Cause Indicates an add port request to a VLAN has failed.

Recommended Action Rerequest to add ports to a VLAN.

Severity ERROR

FCOE-1015

Message `<timestamp>, [FCOE-1015], <sequence-number>,, ERROR, <system-name>, Request to add MACs to L2 for ifindex 0x<ifindex>x failed, rc:<rc>.`

Probable Cause Indicates an add request to L2 for slot or port has failed.

Recommended Action Rerequest to add MACs to L2 for slot/port.

Severity ERROR

FCOE-1016

Message `<timestamp>, [FCOE-1016], <sequence-number>,, ERROR, <system-name>, Request to delete VLAN  <vid> failed.`

Probable Cause Indicates a delete request to delete a VLAN has failed.

Recommended Action The VLAN may be in use; disable the active FCoE login session and try deleting the VLAN again.

Severity ERROR

FCOE-1017

Message `<timestamp>, [FCOE-1017], <sequence-number>,, ERROR, <system-name>, Request to add fcmap failed for vlan <vid>.`

Probable Cause Indicates an add request to VLAN has failed.

Recommended Action When a VLAN is in use, its fcmap is not allowed to be modified. To modify fcmap, disable the active FCoE session on the VLAN.

Severity ERROR

FCOE-1018

Message `<timestamp>, [FCOE-1018], <sequence-number>,, ERROR, <system-name>, Request to delete MACs from L2 for slot/port <portname> failed.`

Probable Cause Indicates a delete request for slot or port has failed.

Recommended Action Rerequest to add MACs from L2 for slot/port.

Severity ERROR

FCOE-1019

Message `<timestamp>, [FCOE-1019], <sequence-number>,, WARNING, <system-name>, FLOGI ignored as FC-MAP not configured on FCOE VLAN.`

Probable Cause Indicates FC-MAP has not been configured on FCOE vlan.

Recommended Action Configure FC-MAP on FCOE vlan.

Severity WARNING

FCOE-1021

Message `<timestamp>, [FCOE-1021], <sequence-number>,, INFO, <system-name>, Port is already logged in.`

Probable Cause Indicates a Nport device has already logged in or is in the process, duplicate FLOGI received.

Recommended Action No action is required.

Severity INFO

FCOE-1022

Message `<timestamp>, [FCOE-1022], <sequence-number>,, WARNING, <system-name>, Max FCoE device login limit reached.`

Probable Cause Indicates that the switch has reached its maximum allowed FCoE device limit.

Recommended Action Do not add any more FCoE devices to the switch.

Severity WARNING

FCOE-1023

Message `<timestamp>, [FCOE-1023], <sequence-number>,, WARNING, <system-name>, Too many logins on FCoE controller, max allowed = <MAX_DEVS_PER_CTLR>.`

Probable Cause Indicates that the controller has reached its maximum allowed FCoE login limit.

Recommended Action No action is required.

Severity WARNING

FCOE-1024

Message `<timestamp>, [FCOE-1024], <sequence-number>,, WARNING, <system-name>, FDISC received from Enode without prior FLOGI.`

Probable Cause Indicates no root Nport has logged in.

Recommended Action No action is required.

Severity WARNING

FCOE-1025

Message `<timestamp>, [FCOE-1025], <sequence-number>,, WARNING, <system-name>, FCOE logout received on FIP VN port.`

Probable Cause Indicates a pre-FIP logout for a device that has logged in using FIP protocol.

Recommended Action It is due to a CNA/target driver issue. No action is required.

Severity WARNING

FCOE-1026

Message `<timestamp>, [FCOE-1026], <sequence-number>,, WARNING, <system-name>, FDISC/FLOGI mismatch. FDISC addressed to different FCF than base FLOGI.`

Probable Cause Indicates the base port has sent an FLOGI but the subsequent FDISC's that was received on the switch does not match the original FLOGI.

Recommended Action It is due to a CNA/target driver issue. No action is required.

Severity WARNING

FCOE-1027

Message `<timestamp>, [FCOE-1027], <sequence-number>,, ERROR, <system-name>, <msg>: <mac1> <mac2> <mac3> <mac4> <mac5> <mac6>.`

Probable Cause Indicates this message is printed if an FDISC is received after an FLOGI but the associated controller cannot be found.

Recommended Action No action is required.

Severity ERROR

FCOE-1028

Message `<timestamp>, [FCOE-1028], <sequence-number>,, ERROR, <system-name>, <msg>: <wwn1> <wwn2> <wwn3> <wwn4> <wwn5> <wwn6> <wwn7> <wwn8>.`

Probable Cause Indicates the FCoE device with following WWN is not a member of the login group : WWN will be printed.

Recommended Action Change the FCoE login group policy on the switch for the device to login.

Severity ERROR

FCOE-1029

Message `<timestamp>, [FCOE-1029], <sequence-number>,, WARNING, <system-name>, Version mismatch between FIP FDISC and root VN port.`

Probable Cause Indicates a version mismatch between the FLOGI and the FDISCs.

Recommended Action No action is required.

Severity WARNING

FCOE-1030

Message `<timestamp>, [FCOE-1030], <sequence-number>,, WARNING, <system-name>, Version mismatch between FIP LOGO and root VN port.`

Probable Cause Indicates a version mismatch between the FIP logout and base FLOGI.

Recommended Action No action is required.

Severity WARNING

FCOE-1031

Message `<timestamp>, [FCOE-1031], <sequence-number>,, WARNING, <system-name>, FCoE port deleted port <prt> slot <slt>.`

Probable Cause Indicates a FCoE port has been deleted.

Recommended Action No action is required.

Severity WARNING

FCOE-1032

Message `<timestamp>, [FCOE-1032], <sequence-number>,, WARNING, <system-name>, We are in WARM RECOVERING state.`

Probable Cause Indicates a HA failover or reboot may be in progress.

Recommended Action No action is required.

Severity WARNING

FCOE-1033

Message `<timestamp>, [FCOE-1033], <sequence-number>,, WARNING, <system-name>, FIP v1 FLOGI received - VF port in use.`

Probable Cause Indicates a device is trying to login to a port that already has something logged in.

Recommended Action No action is required.

Severity WARNING

FCOE-1034

Message `<timestamp>, [FCOE-1034], <sequence-number>,, WARNING, <system-name>, Discarded frame received on priority <pkt_ctrlp->pri_in> for which PFC / FCoE is disabled.`

Probable Cause Indicates the priority PFC/FCoE is not enabled.

Recommended Action Configure as required.

Severity WARNING

FCOE-1035

Message `<timestamp>, [FCOE-1035], <sequence-number>,, INFO, <system-name>, Virtual FCoE port <port number> (<port wwn>) enabled.`

Probable Cause Indicates an administrative action on FCoE port.

Recommended Action No action is required.

Severity INFO

FCOE-1036

Message `<timestamp>, [FCOE-1036], <sequence-number>,, INFO, <system-name>, Virtual FCoE port <port number> (<port wwn>) disabled.`

Probable Cause Indicates an administrative action on FCoE port.

Recommended Action No action is required.

Severity INFO

Chapter

FCPD System Messages

32

FCPD-1001

Message `<timestamp>, [FCPD-1001], <sequence-number>,, WARNING, <system-name>, Probing failed on <error string>.`

Probable Cause Indicates that a Fibre Channel Protocol (FCP) switch probed devices on a loop port, and probing failed on the L_Port, AL_PA address, or the F_Port. For the AL_PA, the valid range is 00 through FF. The error string can be either of the following:

- L_Port *port_number* ALPA *alpa_number*
- F_Port *port_number*

Recommended Action This can happen when the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

Severity WARNING

FCPD-1002

Message `<timestamp>, [FCPD-1002], <sequence-number>,, WARNING, <system-name>, port <port number>, bad R_CTL for fcp probing: 0x<R_CTL value>`

Probable Cause Indicates that the response frame received on the specified port for an inquiry request contains an invalid value in the routing control field.

Recommended Action This can happen only if the firmware on the device controller on the specified port has a defect. Check with the device vendor for a firmware upgrade containing a defect fix.

Severity WARNING

FCPD-1003

Message `<timestamp>, [FCPD-1003], <sequence-number>,, INFO, <system-name>, Probing failed on <error string> which is possibly a private device which is not supported in this port type`

Probable Cause Indicates that private devices will not respond to the switch port login (PLOGI) during probing.

Recommended Action The Brocade DCX, 4100, 4900, 5000, 7500, and AP 7600 do not support private loop devices. Refer to the switch vendor for a list of other port types that support private devices for inclusion into the fabric.

Severity INFO

Chapter

FCPH System Messages

33

FCPH-1001

Message `<timestamp>, [FCPH-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, <function>: <failed function call> failed, out of memory condition`

Probable Cause Indicates that the switch is low on memory and failed to allocate new memory for a Fibre Channel driver instance.

The *function* can only be " fc_create". This function creates a Fibre Channel driver instance.

The *failed function call* kmalloc_wrapper has failed. This function call is for kernel memory allocation.

Recommended Action A nonbladed switch will automatically reboot. For a bladed switch, the active CP blade will automatically fail over and the standby CP will become the active CP.

Severity CRITICAL

FCPH-1002

Message `<timestamp>, [FCPH-1002], <sequence-number>, FFDC, WARNING, <system-name>, Port <Port Number> has been disabled since switch requires authentication when device authentication policy is set to ON.`

Probable Cause Indicates a device which does not support authentication has tried to log in to the switch when the device authentication policy is in ON status on the switch.

Recommended Action Enable the authentication on the device or set the device authentication status to PASSIVE/OFF on the switch if it is not mandatory. Use the **authUtil** command to change the device authentication policy.

Severity WARNING

33 FCPH-1002

Chapter

FCR System Messages

34

FCR-1001

Message `<timestamp>, [FCR-1001], <sequence-number>,, INFO, <system-name>, FC router proxy device in edge created at port <port number>.`

Probable Cause Indicates that a proxy device at the port in the edge fabric has been imported at the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1002

Message `<timestamp>, [FCR-1002], <sequence-number>,, INFO, <system-name>, FC router proxy device in edge deleted at port <port number>.`

Probable Cause Indicates that a proxy device at the port in the edge fabric has been deleted at the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1003

Message `<timestamp>, [FCR-1003], <sequence-number>,, INFO, <system-name>,FC router physical devices newly exported at port <port number>.`

Probable Cause Indicates that one or more physical devices have been newly exported through the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1004

Message `<timestamp>, [FCR-1004], <sequence-number>,, INFO, <system-name>, FC router physical devices offline at port <port number>.`

Probable Cause Indicates that one or more physical devices connected to the specified port have gone offline.

Recommended Action Verify that the devices were intended to be taken offline. If not, verify that the devices are functioning properly. Verify that all small form-factor pluggables (SFPs) are seated correctly. Check for faulty cables, deteriorated SFPs, or dirty connections. Replace the cables and SFPs if necessary.

Severity INFO

FCR-1005

Message `<timestamp>, [FCR-1005], <sequence-number>,, INFO, <system-name>, FC router LSAN zone device removed at port <port number>.`

Probable Cause Indicates that a device is removed from the logical storage area network (LSAN) zone in the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1006

Message `<timestamp>, [FCR-1006], <sequence-number>,, INFO, <system-name>, FC router LSAN zone device added at port <port number>.`

Probable Cause Indicates that a device is added to a logical storage area network (LSAN) zone in the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1007

Message `<timestamp>, [FCR-1007], <sequence-number>,, INFO, <system-name>, FC router LSAN zone deleted at port <port number>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone attached to the specified port was deleted from the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1008

Message `<timestamp>, [FCR-1008], <sequence-number>,, INFO, <system-name>, FC router LSAN zone created at port <port number>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone was created at the specified port in the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1009

Message `<timestamp>, [FCR-1009], <sequence-number>,, INFO, <system-name>, FC router LSAN zone enabled at port <port number>: <enabled name>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone was enabled in the edge fabric attached to the specified port. The enabled LSAN zone configuration is listed.

Recommended Action No action is required.

Severity INFO

FCR-1010

Message `<timestamp>, [FCR-1010], <sequence-number>,, INFO, <system-name>, FC router LSAN zone disabled at port <port number>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone is disabled in the edge fabric attached to the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1011

Message `<timestamp>, [FCR-1011], <sequence-number>,, INFO, <system-name>, Remote LSAN zone updated in domain <domain ID>.`

Probable Cause Indicates that a logical storage area network (LSAN) zone update was received from another domain.

Recommended Action No action is required.

Severity INFO

FCR-1012

Message `<timestamp>, [FCR-1012], <sequence-number>,, INFO, <system-name>, FC Router fabric build completed on port <port number>.`

Probable Cause Indicates that the fibre channel router has completed a fabric build at the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1013

Message `<timestamp>, [FCR-1013], <sequence-number>,, INFO, <system-name>, Phantom FSPF database exchange completed on port <port number>.`

Probable Cause Indicates that the specified EX_Port has completed the fabric shortest path first (FSFP) database exchange.

Recommended Action No action is required.

Severity INFO

FCR-1015

Message `<timestamp>, [FCR-1015], <sequence-number>,, INFO, <system-name>, New EX_Port or VEX_Port added on port <port number> in domain <domain ID>.`

Probable Cause Indicates that an EX _Port was created on the specified port in the specified domain.

Recommended Action No action is required.

Severity INFO

FCR-1016

Message `<timestamp>, [FCR-1016], <sequence-number>,, INFO, <system-name>, FCR fabric no longer reachable at port id <port number> (<port number (hex)>) fabric ID <fabric ID>.`

Probable Cause Indicates that a fabric is no longer accessible through the backbone fabric. This may be caused by a link or switch failure.

Recommended Action No action is required.

Severity INFO

FCR-1018

Message `<timestamp>, [FCR-1018], <sequence-number>,, ERROR, <system-name>, FC router proxy device entries exhausted on port <port number>.`

Probable Cause Indicates that the number of proxy devices is greater than allowed by the port resource.

Recommended Action Remove excess logical storage area network (LSAN) zones or devices until the number of proxy devices exported is within the range allowed by the port resource. Use the **fcrResourceShow** command to view resources including LSAN zone resources, LSAN device resources, and proxy device port resources.

Use the **fcrProxyDevShow** command to view how many proxy devices are created in the fabric with the port resource problem.

LSAN zones are removed using standard zoning commands such as **zoneShow**, **zoneRemove**, **zoneDelete**, **cfgDelete**, and **cfgDisable** in the edge fabric. Proxy devices can be removed by zoning operations or by bringing physical devices offline. For example, disabling the port that a device is attached to, and then disconnecting the cable or disabling the device.

Severity ERROR

FCR-1019

Message `<timestamp>, [FCR-1019], <sequence-number>,, ERROR, <system-name>, EX or VEX port entries exhausted at port <port number>.`

Probable Cause Indicates that the number of EX_Port or VEX_Port entries being created is greater than allowed by the port resource.

Recommended Action EX_Ports or VEX_Ports exceeding the specified range will automatically be disabled by the port resource. Use the **fcrRouteShow** command to display the EX_Port or VEX_Port limits. Use the **portDisable** command to disable EX_Ports.

Severity ERROR

FCR-1020

Message `<timestamp>, [FCR-1020], <sequence-number>,, WARNING, <system-name>, Local LSAN zone entries for FC router exhausted; max limit: <LSAN zone limit>.`

Probable Cause Indicates that the number of logical storage area network (LSAN) zones created within a MetaSAN exceeds the local LSAN zone database limitations.

Recommended Action Remove excess LSAN zones so that the number of LSAN zones created is within the range of local database limitations.

To do that, perform the following steps:

1. Run the **portDisable** command to disable all the EX_Ports that got this error message.
2. Run the **portDisable** command to disable all the other EX_Ports on that FCR connected to the same edge fabrics the EX_ports disabled in step 1 are connected to.

3. Use Zoning commands on the edge fabrics, to reduce the LSAN zone entries on the edge fabrics.
4. Run **portEnable** on each EX_Port, one at a time, and verify that this error is not reported again.

Severity WARNING

FCR-1021

Message `<timestamp>, [FCR-1021], <sequence-number>,, WARNING, <system-name>, Local LSAN device entries exhausted.`

Probable Cause Indicates that the number of devices created through logical storage area network (LSAN) zones within the MetaSAN exceeds the local LSAN zone database limitations.

Recommended Action Remove excess device entries within LSAN zones so that the number of devices is within the range of the local zone database limitations.

Severity WARNING

FCR-1022

Message `<timestamp>, [FCR-1022], <sequence-number>,, ERROR, <system-name>, Local proxy device slot entries exhausted.`

Probable Cause Indicates that the resources used to persistently store the proxy device slot to the remote world wide name (WWN) have been consumed.

Recommended Action Remove the proxy device slots by using the **fcrProxyConfig** command or limit proxy devices by removing logical storage area network (LSAN) zone entries.

Severity ERROR

FCR-1023

Message `<timestamp>, [FCR-1023], <sequence-number>,, WARNING, <system-name>, Local phantom port WWN entries exhausted.`

Probable Cause Indicates that the number of port world wide names (WWNs) in use exceeds the local port WWN resources.

Recommended Action Limit the number of port WWNs required by limiting the remote edge fabric connectivity (which limits the number of translate domains). You can also limit the number of proxy devices for a translate domain (which limits the number of translate domain ports required) by limiting the devices specified in logical storage area network (LSAN) zones.

Severity WARNING

FCR-1024

Message `<timestamp>, [FCR-1024], <sequence-number>,, WARNING, <system-name>, Local LSAN zone <zone name> device entries for edge LSAN exhausted.`

Probable Cause Indicates that the number of devices in a logical storage area network (LSAN) defined in the edge fabric exceeds the local LSAN zone database limitations.

Recommended Action Remove excess device entries from this LSAN zone until the number of devices is within the range of the local LSAN zone database limitations.

Severity WARNING

FCR-1025

Message `<timestamp>, [FCR-1025], <sequence-number>,, WARNING, <system-name>, Local phantom node WWN entries exhausted.`

Probable Cause Indicates that the number of node world wide names (WWNs) detected to be in use exceeds the local node WWN resources.

Recommended Action Reduce the number of node WWNs required by limiting the remote edge fabric connectivity (which limits the number of translate domains).

Severity WARNING

FCR-1026

Message `<timestamp>, [FCR-1026], <sequence-number>,, INFO, <system-name>, In slot <slot number> Node WWN roll over.`

Probable Cause Indicates that the node world wide name (WWN) pool has rolled over in the specified slot, and WWN entries detected to not be in use are reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications.

To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

Severity INFO

FCR-1027

Message `<timestamp>, [FCR-1027], <sequence-number>,, INFO, <system-name>, In slot <slot number> port WWN roll over.`

Probable Cause Indicates that the port world wide name (WWN) pool has rolled over in the specified slot, and WWN entries detected to not be in use are reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications.

To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port or VEX_Port connectivity should be disabled then re-enabled.

Severity INFO

FCR-1028

Message `<timestamp>, [FCR-1028], <sequence-number>,, INFO, <system-name>, In slot <slot number> node WWN pool 95 percent allocated.`

Probable Cause Indicates that the node world wide name (WWN) pool is close to rollover in the specified slot, and that the WWN entries detected not in use will be reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port or VEX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications.

To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

Severity INFO

FCR-1029

Message `<timestamp>, [FCR-1029], <sequence-number>,, INFO, <system-name>, In slot <slot number> port WWN pool 95 percent allocated.`

Probable Cause Indicates that the Port world wide name (WWN) pool has rolled over in the specified slot, and WWN entries detected not in use are reused as needed.

Recommended Action It is unlikely that WWN conflicts will occur as a result of pool rollover unless the switch is deployed in a very large MetaSAN environment with large number of logical storage area network (LSAN) devices and fabrics, or there are highly dynamic changes to EX_Port connectivity. WWN conflicts might cause unpredictable behavior in management applications.

To avoid WWN conflicts, all EX_Ports attached to fabrics with highly dynamic changes to EX_Port connectivity should be disabled and then re-enabled.

Severity INFO

FCR-1030

Message `<timestamp>, [FCR-1030], <sequence-number>,, INFO, <system-name>, Physical device <device WWN> came online at fabric <fabric ID>.`

Probable Cause Indicates that the physical device world wide name (WWN) came online in the specified fabric.

Recommended Action No action is required.

Severity INFO

FCR-1031

Message `<timestamp>, [FCR-1031], <sequence-number>,, INFO, <system-name>, Physical device <device WWN> went offline in fabric <fabric ID>.`

Probable Cause Indicates that the physical device world wide name (WWN) went offline in the specified fabric.

Recommended Action No action is required.

Severity INFO

FCR-1032

Message `<timestamp>, [FCR-1032], <sequence-number>,, INFO, <system-name>, Edge fabric enabled security on port <port number> in fabric <fabric ID>.`

Probable Cause Indicates that Secure mode was turned on in the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1033

Message `<timestamp>, [FCR-1033], <sequence-number>,, INFO, <system-name>, Edge fabric disabled security on port <port number> in fabric <fabric ID>.`

Probable Cause Indicates that Secure mode was turned off in the edge fabric.

Recommended Action No action is required.

Severity INFO

FCR-1034

Message `<timestamp>, [FCR-1034], <sequence-number>,, INFO, <system-name>, LSAN zone added in backbone fabric.`

Probable Cause Indicates that a new logical storage area network (LSAN) zone was added to the backbone fabric.

Recommended Action No action is required.

Severity INFO

FCR-1035

Message `<timestamp>, [FCR-1035], <sequence-number>,, INFO, <system-name>, LSAN zone device added in the backbone fabric.`

Probable Cause Indicates that a new device was added to a logical storage area network (LSAN) zone in the backbone fabric.

Recommended Action No action is required.

Severity INFO

FCR-1036

Message `<timestamp>, [FCR-1036], <sequence-number>,, INFO, <system-name>, LSAN zone <zone name> enabled in the backbone fabric.`

Probable Cause Indicates that the specified logical storage area network (LSAN) zone was enabled in the backbone fabric. The enabled LSAN zone configuration is listed.

Recommended Action No action is required.

Severity INFO

FCR-1037

Message `<timestamp>, [FCR-1037], <sequence-number>,, INFO, <system-name>, LSAN zone disabled in the backbone fabric.`

Probable Cause Indicates that a logical storage area network (LSAN) zone is disabled in the backbone fabric.

Recommended Action No action is required.

Severity INFO

FCR-1038

Message `<timestamp>, [FCR-1038], <sequence-number>,, WARNING, <system-name>, Total zone entries exceeded local fabric limits by <overflow> entries, in zone: <zone name>, zone limit: <LSAN zone limit>.`

Probable Cause Indicates that the number of cfg/zone/alias entries created in a local fabric is greater than the local switch&apos zone database limitations.

Recommended Action Remove excess cfg/zone/alias entries so that the number of logical storage area network (LSAN) zones created is within the range of the local database limitations.

Severity WARNING

FCR-1039

Message `<timestamp>, [FCR-1039], <sequence-number>,, INFO, <system-name>, Local LSAN zone <zone name> device entries for backbone LSAN exhausted.`

Probable Cause Indicates that the number of devices in the specified logical storage area network (LSAN) defined in the backbone fabric is greater than allowed by the local LSAN zone database limitations.

Recommended Action Remove excess device entries from this LSAN zone until the number of devices is within the range of the local LSAN zone database limitations.

Severity INFO

FCR-1040

Message `<timestamp>, [FCR-1040], <sequence-number>,, INFO, <system-name>, Proxy device deleted in the backbone fabric.`

Probable Cause Indicates that a proxy device created in the backbone fabric was deleted.

Recommended Action No action is required.

Severity INFO

FCR-1041

Message `<timestamp>, [FCR-1041], <sequence-number>,, INFO, <system-name>, LSAN zone device removed in the backbone fabric.`

Probable Cause Indicates that a logical storage area network (LSAN) zone device within the backbone fabric was removed.

Recommended Action No action is required.

Severity INFO

FCR-1042

Message `<timestamp>, [FCR-1042], <sequence-number>,, INFO, <system-name>, LSAN zone removed in the backbone fabric.`

Probable Cause Indicates that a logical storage area network (LSAN) zone within the backbone fabric was removed.

Recommended Action No action is required.

Severity INFO

FCR-1043

Message `<timestamp>, [FCR-1043], <sequence-number>,, INFO, <system-name>, Proxy device created in the backbone fabric.`

Probable Cause Indicates that a proxy device was created in the backbone fabric.

Recommended Action No action is required.

Severity INFO

FCR-1048

Message `<timestamp>, [FCR-1048], <sequence-number>,, ERROR, <system-name>, On EX port (<port number>) setting port <credit type> credits failed.`

Probable Cause Indicates that the specified *credit type* was not set.

Recommended Action Setting port credits failed. Execute the **portEnable** command.

If the problem persists try restarting the switch.

If the message persists, collect switch information using the **supportShow** command, and contact your switch service provider.

Severity ERROR

FCR-1049

Message `<timestamp>, [FCR-1049], <sequence-number>,, ERROR, <system-name>, EX port (<port number>) received an ELP command that is not supported.`

Probable Cause Indicates an incoming exchange link protocol (ELP) command was issued and it is not supported.

Recommended Action Run the **portEnable** and **portDisable** commands to enable and disable the port.

If the problem persists contact your switch service provider.

Severity ERROR

FCR-1053

Message `<timestamp>, [FCR-1053], <sequence-number>,, WARNING, <system-name>, Port <port number> was disabled, <disable reason>.`

Probable Cause Indicates that the specified port was disabled because of a mismatched configuration parameter.

Recommended Action Use the specified *disable reason* to identify a possible configuration parameter mismatch between the EX_Port and the switch at other end of the link.

Severity WARNING

FCR-1054

Message `<timestamp>, [FCR-1054], <sequence-number>,, WARNING, <system-name>, Port <port number> received ILS <command> of incorrect size (<actual payload size>); valid ILS size is <expected payload size>.`

Probable Cause Indicates that an internal link service (ILS) IU of invalid size was received from the switch on the other end of the link.

Recommended Action Check the error message log on the other switch using the **errShow** command for additional messages.

Check for a faulty cable or deteriorated small form-factor pluggable (SFP). Replace the cable or SFP if necessary.

Run the **portLogDumpPort** command on both the receiving and transmitting port.

Run the **fabStateShow** command on the transmitting switch.

If the message persists, collect switch information using the **supportShow** command, and contact your switch service provider.

Severity WARNING

FCR-1055

Message `<timestamp>, [FCR-1055], <sequence-number>,, INFO, <system-name>, Switch with domain ID <domain ID> does not support backbone to edge imports.`

Probable Cause Indicates that a switch that does not support backbone-to-edge routing was detected in the backbone. Edge-to-edge routing will work, but backbone-to-edge routing might fail.

Recommended Action No action is required if backbone to edge routing is not required. Otherwise replace the switch with one that supports backbone to edge routing.

Severity INFO

FCR-1056

Message `<timestamp>, [FCR-1056], <sequence-number>,, INFO, <system-name>, Switch <switch WWN> with front domain ID <domain ID> does not support backbone to edge imports.`

Probable Cause Indicates that a switch that does not support backbone-to-edge routing is running in the MetaSAN.

Recommended Action No action is required if backbone-to-edge routing is not needed. Otherwise replace the switch with one that supports backbone to edge routing.

Severity INFO

FCR-1057

Message `<timestamp>, [FCR-1057], <sequence-number>,, ERROR, <system-name>, EX_Port(<port number>) incompatible long distance parameters on link.`

Probable Cause Indicates that the port, which is configured in long distance mode, has incompatible long distance parameters.

Recommended Action Check the port configuration on both sides of the link using the **portCfgShow** command.

Investigate the other switch for more details. Run the **errShow** command on the other switch to view the error log for additional messages.

Severity ERROR

FCR-1058

Message `<timestamp>, [FCR-1058], <sequence-number>,, WARNING, <system-name>, Port <port number> isolated due to mismatched configuration parameter; <segmentation reason>.`

Probable Cause Indicates that the specified port was isolated after segmentation caused by mismatched configuration parameters or by domain ID assigned by the principal switch that did not match the insistent domain ID of this port.

Recommended Action Check the switches on both ends of the link for a possible mismatch in switch or port configuration parameters such as Operating Mode, E_D_TOV, R_A_TOV, Domain ID Offset, etc.

Run the **portCfgExport** command to modify the appropriate parameters on the local switch.

Run the appropriate configuration command to modify the switch or port parameters on the remote switch.

Severity WARNING

FCR-1059

Message `<timestamp>, [FCR-1059], <sequence-number>,, INFO, <system-name>, EX_Port <port number> was disabled due to an authentication failure.`

Probable Cause Indicates that the authentication, which uses the Diffie Hellman - challenge handshake authentication Protocol (DH-CHAP), failed on the EX_Port.

Recommended Action Verify that the shared secrets on both sides of the link match.

Disable and enable the ports by using the **portDisable** and the **portEnable** commands to restart authentication.

Severity INFO

FCR-1060

Message `<timestamp>, [FCR-1060], <sequence-number>,, WARNING, <system-name>, EX_Port(<port number>) has an incompatible configuration setting.`

Probable Cause Indicates that virtual channel (VC) Link Init is enabled on the local switch and the remote switch is negotiating in R_RDY mode. The fabric might not form properly.

Recommended Action Check the configuration on the local switch using the **portCfgShow** command to verify that the VC Link Init is disabled, if the remote switch is configured in R_RDY mode or only capable of R_RDY mode.

VC_RDY mode: Virtual-channel flow control mode. This is a proprietary protocol.

R_RDY mode: Receiver-ready flow control mode. This is the Fibre Channel standard protocol, that uses R_RDY primitive for flow control.

Severity WARNING

FCR-1061

Message `<timestamp>, [FCR-1061], <sequence-number>,, INFO, <system-name>, Backbone fabric created on port <port number>.`

Probable Cause Indicates that a backbone fabric was built on the specified port.

Recommended Action No action is required.

Severity INFO

FCR-1062

Message `<timestamp>, [FCR-1062], <sequence-number>,, INFO, <system-name>, Port <port number> disabled, system only supports <maximum ports> EX/VEX_ports.`

Probable Cause Indicates that the maximum number of supported EX_ports or VEX_ports was exceeded. To enable the specified port, disable any other operational port then re-enable the port.

Recommended Action No action is required.

Severity INFO

FCR-1063

Message `<timestamp>, [FCR-1063], <sequence-number>,, INFO, <system-name>, Fabric <fabric ID> for switch with domain ID: <domain ID> mismatch with local fabric ID <local fabric ID>.`

Probable Cause Indicates that the fabric ID of the switch does not match the local switch.

Recommended Action Run the **switchShow** command to display the fabric ID. Change the fabric ID to match on both ends by modifying either the local or remote host using the **fcrConfigure** command.

Severity INFO

FCR-1064

Message `<timestamp>, [FCR-1064], <sequence-number>,, ERROR, <system-name>, Fabric ID of backbone FC-Routers mismatch or overlap.`

Probable Cause Indicates that either (1) a backbone fabric split and both are connected to common edge fabrics, or (2) the fabric IDs of two backbone fabrics connected to an edge fabric are the same.

Recommended Action If the backbone fabric split, merge the fabrics.

If two (or more) backbone fabrics have the same IDs, make the fabric IDs unique using **fcrConfigure** command.

Severity ERROR

FCR-1065

Message `<timestamp>, [FCR-1065], <sequence-number>,, ERROR, <system-name>, Fabric on port <port number> was assigned two different fabric IDs.`

Probable Cause Indicates that another port on the switch is connected to the same edge fabric with a different fabric ID assignment.

Recommended Action Change the port fabric ID to same value as the other ports connected to the edge fabric using the **portCfgExport** or **portCfgVexport** commands.

Severity ERROR

FCR-1066

Message `<timestamp>, [FCR-1066], <sequence-number>,, ERROR, <system-name>, Fabric on port <port number> has the same fabric ID as another fabric.`

Probable Cause Indicates that either the fabric split, or there is another fabric (possibly the backbone) that has the same fabric ID as the fabric connected to the specified port.

Recommended Action If the fabric split, then merge the fabrics and manually re-enable the port.

If there is another fabric with the same ID, change the fabric ID for the port using the **portCfgExport** or **portCfgVExport** commands.

Severity ERROR

FCR-1067

Message `<timestamp>, [FCR-1067], <sequence-number>,, WARNING, <system-name>, Zone configurations, total LSAN zones and aliases, exceeded on port <port number> by <overflow> entries; max entries: <LSAN zone limit>.`

Probable Cause Indicates that the total number of zone configurations created in the connected fabric exceeds the maximum number supported by the Fibre Channel.

The limit includes both active and configured information that is part of the zoning database in the edge fabric. Non-LSAN zones are not counted in the limit.

Recommended Action Limit the logical storage area network (LSAN) zoning related zone configuration in the edge fabric connected to this port.

Severity WARNING

FCR-1068

Message `<timestamp>, [FCR-1068], <sequence-number>,, INFO, <system-name>, The FC Routing service is disabled.`

Probable Cause Indicates that the FC Routing service is disabled. This is caused by **fosConfig --disable fcr, configDefault**, or a **configDownload** with the **fcrState** set to 2 (disabled). Note that the FC Routing service is disabled by the factory.

Recommended Action No action is required.

Severity INFO

FCR-1069

Message `<timestamp>, [FCR-1069], <sequence-number>,, INFO, <system-name>, The FC Routing service is enabled.`

Probable Cause Indicates that the FC Routing service is enabled. This is caused by either **fosConfig --enable** fcr, or a **configDownload** with the **fcrState** set to 1 (enabled). Note that the FC Routing service is disabled by the factory.

Recommended Action No action is required.

Severity INFO

FCR-1070

Message `<timestamp>, [FCR-1070], <sequence-number>,, INFO, <system-name>, The FC Routing configuration is set to default.`

Probable Cause Indicates that the FC Routing configuration is set to default by user. This removes all prior FC Routing configurations.

Recommended Action No action is required.

Severity INFO

FCR-1071

Message `<timestamp>, [FCR-1071], <sequence-number>,, INFO, <system-name>, Port <port number> is changed from non FCR port to FCR port.`

Probable Cause Indicates that the port became an EX_Port or VEX_Port.

Recommended Action No action is required.

Severity INFO

FCR-1072

Message `<timestamp>, [FCR-1072], <sequence-number>,, INFO, <system-name>, Port <port number> is changed from FCR port to non FCR port.`

Probable Cause Indicates that the port is no longer an EX_Port or VEX_Port.

Recommended Action No action is required.

Severity INFO

FCR-1073

Message `<timestamp>, [FCR-1073], <sequence-number>,, INFO, <system-name>, Switch with domain ID <domain ID> in fabric <fabric ID> has lower limit of LSAN Zones supported.`

Probable Cause Indicates that an earlier version of the switch in the backbone or edge that supports a different limit of logical storage area network (LSAN) zones was detected.

Recommended Action Use the **fcrResourceShow** command on all Fibre Channel Routers in the Meta-SAN to find the lowest supported LSAN zone limits. Ensure that total number of LSAN zones in the Meta-SAN are within the lowest supported limit of LSAN zones.

Severity INFO

FCR-1074

Message `<timestamp>, [FCR-1074], <sequence-number>,, ERROR, <system-name>, HA sync lost as remote CP supports only <LSAN count> LSAN Zones.`

Probable Cause Indicates that the remote control processor (CP) has older firmware, which only supports a lower number of logical storage area network (LSAN) zones. This is causing the loss of the high-availability (HA) sync.

Recommended Action Keep the number of LSAN Zones to the lower limit of the two CPs or upgrade the remote CP.

Severity ERROR

FCR-1075

Message `<timestamp>, [FCR-1075], <sequence-number>,, ERROR, <system-name>, Zone Name configuration is larger than <Zone Name Limit> characters in the edge fabric connected to port <port numer>.`

Probable Cause Indicates that the zone name configuration size created in the connected fabric exceeds the maximum supported by the FC Router. This size is equal to the total number of characters used by all the zone names in the edge fabric zoning database.

The limit includes both logical storage area network (LSAN) and Non-LSAN zone names defined in zoning name database of the edge fabric.

Recommended Action Limit the zone configuration size in the edge fabric connected to this port by either reducing number of zones or changing the zone names to smaller names.

Severity ERROR

FCR-1076

Message `<timestamp>, [FCR-1076], <sequence-number>,, ERROR, <system-name>, Port <port number> disabled, system only supports <maximum fds> front domains.`

Probable Cause Indicates that the maximum number of supported front domains was exceeded. To enable the specified port, disable any other operational front domain and then re-enable the port.

Recommended Action Make sure to remain within the maximum of supported front domains.

Severity ERROR

FCR-1077

Message `<timestamp>, [FCR-1077], <sequence-number>,, WARNING, <system-name>, Port <port number> rejected fabric binding request/check from the M-Model switch; <port number>.`

Probable Cause Indicates that an M-Model edge switch attempted to either activate or check the fabric binding. This port will be disabled if this event occurred during a check of fabric binding and not during failure to activate fabric binding. The error is caused when the binding list details configured on the M-Model switch does not match with the currently configured front port domain ID and WWN of the EX_Port on which this operation was attempted.

Recommended Action Ensure that the M-Model switch has the same currently configured details such as front port domain ID and WWN of the EX_Port on which this operation was attempted.

Severity WARNING

FCR-1078

Message `<timestamp>, [FCR-1078], <sequence-number>,, WARNING, <system-name>, LSAN name <LSAN name> is too long. It is dropped.`

Probable Cause Indicates that the length of the LSAN name exceeds the limit of 64 characters.

Recommended Action Change the name and reactivate the zone database.

Severity WARNING

FCR-1079

Message `<timestamp>, [FCR-1079], <sequence-number>,, WARNING, <system-name>, Domain <Domain> has conflict matrix database with local domain.`

Probable Cause Indicates that the specified domain has a different matrix database from the local domain.

Recommended Action Change the matrix database.

Severity WARNING

FCR-1080

Message `<timestamp>, [FCR-1080], <sequence-number>,, WARNING, <system-name>, The pause response timer for domain <Domain> expired.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has not responded to the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the result of the rejected pause message.

Recommended Action No action is required.

Severity WARNING

FCR-1081

Message `<timestamp>, [FCR-1081], <sequence-number>,, WARNING, <system-name>, The pause message is rejected by the domain <Domain>.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected pause message.

Recommended Action No action is required.

Severity WARNING

FCR-1082

Message `<timestamp>, [FCR-1082], <sequence-number>,, WARNING, <system-name>, The pause retry count is exhausted for the domain <Domain>.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action No action is required.

Severity WARNING

FCR-1083

Message `<timestamp>, [FCR-1083], <sequence-number>,, WARNING, <system-name>, The resume message is rejected by the domain <Domain>.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric has rejected the pause message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to the rejected resume message.

Recommended Action No action is required.

Severity WARNING

FCR-1084

Message `<timestamp>, [FCR-1084], <sequence-number>,, WARNING, <system-name>, The resume retry count is exhausted for the domain <Domain>.`

Probable Cause Indicates that during the Coordinated HotCode protocol, a switch in the fabric did not accept the resume message which prevented the protocol from completing. Any data traffic disruption observed during the firmware download may have been due to this issue.

Recommended Action No action is required.

Severity WARNING

FCR-1085

Message `<timestamp>, [FCR-1085], <sequence-number>,, ERROR, <system-name>, HA sync lost as remote CP does not support FCR based matrix.`

Probable Cause Indicates that the remote control processor (CP) has earlier firmware, which does not support the FCR- based matrix while the local CP has the feature enabled. This is causing the loss of the high-availability (HA) synchronization.

Recommended Action Disable FCR-based matrix or upgrade the remote CP.

Severity ERROR

FCR-1086

Message `<timestamp>, [FCR-1086], <sequence-number>,, ERROR, <system-name>, HA sync lost as remote CP does not support Condor2 based EX_ports.`

Probable Cause Indicates that the remote control processor (CP) has older firmware, which does not support Condor-based EX_ port. This is causing the loss of the high-availability (HA) synchronization.

Recommended Action Disable Condor2-based EX_ports or upgrade the remote CP.

Severity ERROR

FCR-1087

Message `<timestamp>, [FCR-1087], <sequence-number>,, ERROR, <system-name>, ExPort <ExPort> connects to fabric <fabric> with capability to use XISL domain <domain>.`

Probable Cause Indicates that the EX_Port connects to logical fabric containing a domain has the capability to use XISL.

Recommended Action Disable the 'Allow to use XISL' mode of the domain by using the **configure** command.

Severity ERROR

FCR-1088

Message `<timestamp>, [FCR-1088], <sequence-number>,, INFO, <system-name>, LSAN <Enforce/Speed> tag <Tag Name> added.`

Probable Cause Indicates that the user has added a LSAN tag.

Recommended Action No action is required.

Severity INFO

FCR-1089

Message `<timestamp>, [FCR-1089], <sequence-number>,, INFO, <system-name>, LSAN <Enforce/Speed> tag <Tag Name> removed.`

Probable Cause Indicates that the user has added a LSAN tag.

Recommended Action No action is required.

Severity INFO

FCR-1091

Message `<timestamp>, [FCR-1089], <sequence-number>,, INFO, <system-name>, Backbone Fabric ID changed to <Tag>.`

Probable Cause Indicates that the backbone fabric ID has been changed.

Recommended Action No action is required.

Severity INFO

FCR-1092

Message `<timestamp>, [FCR-1089], <sequence-number>,, ERROR, <system-name>, FCR ELS trap entries exhausted.`

Probable Cause Indicates that the FCR ELS trap entries are exhausted.

Recommended Action Collect **supportsave** data and send it to support.

Severity ERROR

Chapter

FICON System Messages

35

The FICON messages in this chapter include **<FICON Path>** in many of the messages. The FICON Path is a string that includes, **VEHDHPDDDPLPCUDV** where:

VE - VE Port Number: This number represents the FCIP Tunnel number through its VE Port number.

HD - Host switch Domain number: This is a 1 byte hexidecimal value that represents the domain of the switch that the FICON Channel is directly connected to.

HP - Host Port number: This is a 1 byte hexidecimal value that represents the switch port of the switch that the FICON Channel is directly connected to.

DD - Device Domain number: This is a 1 byte hexidecimal value that represents the domain of the switch that the FICON Control Unit is directly connected to.

DP - Device Port number: This is a 1 byte hexidecimal value that represents the switch port of the switch that the FICON Control Unit is directly connected to.

LP - Host LPAR number: This is a 1 byte hexidecimal value that represents the Logical Partition or Logical Channel Number used on the FICON connection.

CU - CU Number: This is a 1 byte hexidecimal value that is the Logical Control Unit number (AKA CUADDR) - normally a value in the range of 00-0x1F.

DV - Device Number: This is a 1 byte hexidecimal value that is the Logical Control Unit number (AKA CUADDR) - normally a value in the range of 00-0xFF

Note that there are some messages where the lower order FICON Path components can be displayed as "**" in those cases, the event or message applicability is not limited to a Device Number or Control Unit or LPAR. Those messages would include the following format of the FICON Path:

VEHDHPDDDPLPCU** - indicates that the event or message is specific to all Devices on a specific Control Unit.

VEHDHPDDDPLP**** - indicates that the event or message is specific to all Control Units and all Devices on those control Units from a specific LPAR.

VEHDHPDDDP****** - indicates that the event or message is specific to all Control Units and all Devices on those control Units from a all LPARs on that FICON Channel.

FICN-1003

Message <timestamp>, [FICN-1003], <sequence-number>,, WARNING, <system-name>, FICON Tape Emulation License Key is not installed.

Probable Cause Indicates FICON Tape Emulation requires a License Key.

Recommended Action Use the appropriate License Key.

Severity WARNING

FICN-1004

Message `<timestamp>, [FICN-1004], <sequence-number>,, WARNING, <system-name>, FICON XRC Emulation License Key is not installed.`

Probable Cause Indicates FICON XRC Emulation requires a License Key.

Recommended Action Use the appropriate License Key.

Severity WARNING

FICN-1005

Message `<timestamp>, [FICN-1005], <sequence-number>,, INFO, <system-name>, FICON GEPort <GE port number> TID <tunnel number> Feature Change verified Xrc <1 or 0 - XRC Emulation Enabled or Disabled> TapeWrt <1 or 0 - Tape Write Emulation Enabled or Disabled> TapeRd <1 or 0 - FICON Tape Read Emulation Enabled or Disabled> TinTir <1 or 0 - FICON TIN/TIR Emulation Enabled or Disabled> DvcAck <1 or 0 - FICON Device Level Ack Emulation Enabled or Disabled> RdBlkId <1 or 0 - FICON Write Emulation Read Block ID Emulation Enabled or Disabled>.`

Probable Cause Indicates the configuration was changed manually.

Recommended Action No action is required.

Severity INFO

FICN-1006

Message `<timestamp>, [FICN-1006], <sequence-number>,, WARNING, <system-name>, FICON GEPort < 0 or 1 - GE port number> TID <Tunnel Number> Feature Change failed Xrc <1 or 0 - FICON XRC Emulation Enabled or Disabled> TapeWrt <1 or 0 - Tape Write Emulation Enabled or Disabled> TapeRd <1 or 0 - FICON Tape Read Emulation Enabled or Disabled> TinTir <1 or 0 - FICON TIN/TIR Emulation Enabled or Disabled> DvcAck <1 or 0 - FICON Device Level Ack Emulation Enabled or Disabled> RdBlkId <1 or 0 - FICON Write Emulation Read Block ID Emulation Enabled or Disabled>.`

Probable Cause Indicates the FCIP Tunnel ID associated with the FICON tunnel must be down or disabled for a feature change to become effective.

Recommended Action Disable the applicable FCIP tunnel to make the feature change effective.

Severity WARNING

FICN-1007

Message `<timestamp>, [FICN-1007], <sequence-number>,, ERROR, <system-name>, DevDiskEgr:FICON Selective Reset:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> State=0x<current Emulation State> stat_array=0x<last 4 Status values that were received from the device>.`

Probable Cause Indicates a Selective Reset from the channel was received as either a normal part of path recovery or starting sequence in an error case.

Recommended Action If there was a job failure associated with this event, please contact your vendor's customer support.

Severity ERROR

FICN-1008

Message `<timestamp>, [FICN-1008], <sequence-number>,, ERROR, <system-name>, DevDiskEgr:FICON Purge Path received Path=<VEPortNumber HostDomain HostPort DeviceDomcontactain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates a FICON Purge Path was received from the channel as a part of path recovery.

Recommended Action If there was a job failure associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1009

Message `<timestamp>, [FICN-1009], <sequence-number>,, INFO, <system-name>, DevIng:CmdReject Sense Data rcvd:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> <Current Emulation State> LastCmds=<the Last 4 commands issued to the device> Sense Data:Bytes0-0xB=<bytes 0-3 of sense data from the device> <bytes 4-7 of sense data from the device> <bytes 8-0x0b of sense data from the device>.`

Probable Cause Indicates a Unit Check status was received from a device and a sense command was issued to read the sense data.

Recommended Action If there was a job failure associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1010

Message `<timestamp>, [FICN-1010], <sequence-number>,, INFO, <system-name>, DevDiskEgr:Device level exception flag found for Path=<VEPortNumber HostDomain HostPort DeviceDomain>8X<DevicePort LPAR CUADDR DeviceAddr>8X: Oxid=0x<The OXID that was reported in the Device Level Exception Frame>4X.`

Probable Cause Indicates a Device Level Exception frame was received from the FICON Channel.

Recommended Action If there was a job or IO failure associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1011

Message

```
<timestamp>, [FICN-1011], <sequence-number>,, ERROR, <system-name>,
DevDiskIng:XRC Incorrect RRS SeqNum Rcvd Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain>8X<DevicePort LPAR CUADDR DeviceAddr>8X Expected=0x<The RRS Sequence
number that was expected from the device>4X Received=0x<The RRS Sequence number
that was actually received from the device>4X Oxid=0x<The data frame's OXID>4X.
```

Probable Cause Indicates the Control Unit/device presented a Read Record Set Sequence number different from the SDM's expected sequence number.

Recommended Action If there was an XRC volume or session suspended associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1012

Message

```
<timestamp>, [FICN-1012], <sequence-number>,, ERROR, <system-name>,
DevDiskIng:Device level exception found for Path=0x<VEPortNumber HostDomain
HostPort DeviceDomain>8X<DevicePort LPAR CUADDR DeviceAddr>8X: Oxid=0x<The OXID
that was reported in the Device Level Exception Frame>4X.
```

Probable Cause Indicates a Device Level Exception frame received from the FICON DASD Control Unit.

Recommended Action If there was a job or IO failure associated with this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1013

Message

```
<timestamp>, [FICN-1013], <sequence-number>,, INFO, <system-name>,
DevDiskIng:Status=0x<Status that was received from the DASD device in an odd
state>2X received in odd state=0x<The current emulation state>2X from
Path=0x<VEPortNumber HostDomain HostPort DeviceDomain>8X<DevicePort LPAR CUADDR
DeviceAddr>8X sent LBY.
```

Probable Cause Indicates that when the device sent the status in an incorrect state, the emulation processing rejected the status with an LBY frame.

Recommended Action If there was a job or IO failure associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1014

Message `<timestamp>, [FICN-1014], <sequence-number>,, INFO, <system-name>, DevEgr:Device level exception flag found for Path=0x<VEPortNumber HostDomain HostPort DeviceDomain>8X<DevicePort LPAR CUADDR DeviceAddr>8X: Oxid=0x<The OXID used to deliver the non-AS Device Level Exception>4X.`

Probable Cause Indicates a frame was received that indicated device level exception.

Recommended Action If there was an IO failure associated with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1015

Message `<timestamp>, [FICN-1015], <sequence-number>,, ERROR, <system-name>, DevEgr:cuPath=0x<VEPortNumber HostDomain HostPort DeviceDomain>8X******:Discarding Invalid LRCd SOF=0x<The invalid Frame's SOF value (SOFiX or SOFnx)>8X count=<The total number of frames that have been received from the peer with incorrect FICON LRC values>.`

Probable Cause Indicates a frame was received from the peer emulation processing with an invalid LRC. This indicates data corruption between the emulation processing components.

Recommended Action Please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1016

Message `<timestamp>, [FICN-1016], <sequence-number>,, INFO, <system-name>, DevIng:Received Logical Path Removed response:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain>8X<DevicePort LPAR>4X<CUADDR>2X.`

Probable Cause Indicates the FICON Control Unit sent an LPR frame to the FICON channel.

Recommended Action This is an informational message and does not require any action.

Severity INFO

FICN-1017

Message `<timestamp>, [FICN-1017], <sequence-number>,, INFO, <system-name>, DevIng:Received Logical Path Established response:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain>8X<DevicePort LPAR>4X<CUADDR>2X.`

Probable Cause Indicates the FICON Control Unit sent an LPE frame to the FICON channel.

Recommended Action This is an informational message and does not require any action.

Severity INFO

FICN-1018

Message
```
<timestamp>, [FICN-1018], <sequence-number>,, ERROR, <system-name>, DevIng:FCUB
Lookup failed for Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain>8x<DevicePort LPAR>2x.
```

Probable Cause Indicates the FICON Control Unit sent a frame that cannot be associated with a FICON Control Unit CUADDR.

Recommended Action Contact your vendor's customer support for assistance.

Severity ERROR

FICN-1019

Message
```
<timestamp>, [FICN-1019], <sequence-number>,, ERROR, <system-name>, DevTapeEgr:AS
Link Level Reject (LRJ) from Chan on Path=0x<VEPortNumber HostDomain HostPort
DeviceDomain>8X<DevicePort LPAR CUADDR DeviceAddr>8X LastCmd=0x<the Last 4
commands issued to the device>8x LastStatus=0x<the Last 4 status values received
from the device>8x.
```

Probable Cause Indicates the FICON channel indicated in the path issued an LRJ frame for a sequence from the device.

Recommended Action If there was a job failure associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1020

Message
```
<timestamp>, [FICN-1020], <sequence-number>,, ERROR, <system-name>,
DevTapeEgr:FICON Cancel received Path=<VEPortNumber HostDomain HostPort
DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> state=0x<the current emulation
state for the device>2X tflags=0x<the current emulation tape control flags for the
device>8X sflags=0x<the current emulation status control flags for the device>4X.
```

Probable Cause Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1021

Message `<timestamp>, [FICN-1021], <sequence-number>,, ERROR, <system-name>, DevTapeEgr:FICON Tape Cancel:Path=0x<VEPortNumber HostDomain HostPort DeviceDomain>8X<DevicePort LPAR CUADDR DeviceAddr>8X Elapsed Time=<the current SIO time in seconds for the device>.<the current SIO time in milliseconds for the device> seconds.`

Probable Cause Indicates the FICON channel issued a Cancel sequence for a device in emulation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1022

Message `<timestamp>, [FICN-1022], <sequence-number>,, ERROR, <system-name>, DevTapeEgr:FICON Selective Reset:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> State=0x<the current state of the device that received the selective reset> statArray=0x<the last 4 status values received from the device> cmdArray=0x<the last 4 commands that were issued to the device> tflags=0x<the current emulation tape control flags for the device> sflags=0x<the current emulation status control flags for the device>.`

Probable Cause Indicates the FICON channel issued a Selective Reset for a device that was active in emulation.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1023

Message `<timestamp>, [FICN-1023], <sequence-number>,, ERROR, <system-name>, DevTapeEgr:FICON Selective Reset:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> Elapsed Time=<the current SIO time in seconds for the device>.<the current SIO time in milliseconds for the device> seconds.`

Probable Cause Indicates the FICON channel issued a Selective Reset sequence for a device.

Recommended Action If there was an unexpected job failure associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1024

Message `<timestamp>, [FICN-1024], <sequence-number>,, ERROR, <system-name>, DevTapeEgr:FICON Purge received Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates the FICON channel issued a Purge Path command sequence for a device.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1025

Message `<timestamp>, [FICN-1025], <sequence-number>,, ERROR, <system-name>, DevTapeIng:Auto Sense Data received on Path=0x<VEPortNumber HostDomain HostPort DeviceDomain>8X<DevicePort LPAR CUADDR DeviceAddr>8X Bytes0-0xB=0x<bytes 0-3 of sense data from the device>8X<bytes 4-7 of sense data from the device>8X<bytes 8-0x0b of sense data from the device>8X.`

Probable Cause Indicates the FICON tape write pipelining processed sense data from a FICON device.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1026

Message `<timestamp>, [FICN-1026], <sequence-number>,, INFO, <system-name>, DevTapeIng:UnusualStatus:WriteCancelSelr:Generating Final Ending Status Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates the FICON tape write pipeline is completing an emulated Selective Reset sequence.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, contact your vendor's customer support for assistance.

Severity INFO

FICN-1027

Message `<timestamp>, [FICN-1027], <sequence-number>,, ERROR, <system-name>, DevTapeIng:Device level exception found for Path=<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR CUADDR DeviceAddr>: Oxid=0x<The OXID of the frame that included the Device Level Exception>.`

Probable Cause Indicates an active emulation device delivered a Device Level Exception frame to the emulation processing.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1028

Message `<timestamp>, [FICN-1028], <sequence-number>,, ERROR, <system-name>, HostDiskIng:FICON Cancel received Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>state=0x<The current emulation state of the device>.`

Probable Cause Indicates an active emulation device received a cancel operation from the FICON channel.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1029

Message `<timestamp>, [FICN-1029], <sequence-number>,, ERROR, <system-name>, HostDiskIng:FICON Selective Reset:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>state=0x<The current emulation state of the device> LastCmds=0x<The last 4 commands received from the channel for this device> LastStatus=0x<The last 4 status values presented to the channel for this device>.`

Probable Cause Indicates an active disk emulation device received a Selective Reset from the FICON channel.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1030

Message `<timestamp>, [FICN-1030], <sequence-number>,, ERROR, <system-name>, HostDiskIng:FICON Purge received:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates an active disk emulation device received a FICON Purge Path from the channel.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1031

Message `<timestamp>, [FICN-1031], <sequence-number>,, WARNING, <system-name>, HostDiskIng:FICON System Reset received on Path=<VEPortNumber HostDomain HostPort DeviceDomain><DevicePort LPAR><CUADDR>.`

Probable Cause Indicates the FICON channel sent a System Reset to the disk control unit.

Recommended Action No action is required. The MVS system was either set to IPL or performing error recovery.

Severity WARNING

FICN-1032

Message `<timestamp>, [FICN-1032], <sequence-number>,, INFO, <system-name>, HostDiskIng:XRC Read Channel Extender Capabilities detected on Path: <VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates the XRC System Data mover was restarted to discover the capabilities of the channel extension equipment.

Recommended Action No action is required. This is a part of the XRC initialization.

Severity INFO

FICN-1033

Message `<timestamp>, [FICN-1033], <sequence-number>,, INFO, <system-name>, HostEgr:Logical Path Established on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR> <CUADDR>.`

Probable Cause Indicates the peer side FICON Control Unit has accepted a logical path establishment command sequence with the FICON channel.

Recommended Action No action is required. This is a part of the FICON path initialization.

Severity INFO

FICN-1034

Message `<timestamp>, [FICN-1034], <sequence-number>,, ERROR, <system-name>, HostEgr:Discarding Invalid LRCd Frame on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort> count=<The total number of frames that have been received with an invalid LRC>.`

Probable Cause Indicates the channel emulation processing received a frame with an invalid FICON LRC from the peer. This indicates that the channel side noted corruption from the device/CU side processing.

Recommended Action Contact your vendor's customer support for assistance.

Severity ERROR

FICN-1035

Message `<timestamp>, [FICN-1035], <sequence-number>,, WARNING, <system-name>, HostIng:FICON System Reset received on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort> <LPAR> <CUADDR>.`

Probable Cause Indicates a locally connected FICON channel issued a System Reset to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path initialization.

Severity WARNING

FICN-1036

Message `<timestamp>, [FICN-1036], <sequence-number>,, INFO, <system-name>, HostIng:FICON RLP Request on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort> <LPAR> <CUADDR>.`

Probable Cause Indicates a locally connected FICON Channel issued a Remove Logical Path sequence to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path deactivation.

Severity INFO

FICN-1037

Message `<timestamp>, [FICN-1037], <sequence-number>,, INFO, <system-name>, HostIng:FICON ELP Request on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort> <LPAR> <CUADDR>.`

Probable Cause Indicates a locally connected FICON Channel issued an Establish Logical Path sequence to the specified FICON Control Unit.

Recommended Action No action is required. This is a part of the FICON path activation.

Severity INFO

FICN-1038

Message `<timestamp>, [FICN-1038], <sequence-number>,, ERROR, <system-name>, fcFicIngHost:FDCB Lookup failed for Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort>.`

Probable Cause Indicates a locally connected FICON channel sent a frame that could not be associated with a FICON device.

Recommended Action Contact your vendor's customer support for assistance.

Severity ERROR

FICN-1039

Message `<timestamp>, [FICN-1039], <sequence-number>,, ERROR, <system-name>, HostIng:FCUB Lookup failed for Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR>.`

Probable Cause Indicates a locally connected FICON channel sent a frame that could not be associated with a FICON Control Unit.

Recommended Action Contact your vendor's customer support for assistance.

Severity ERROR

FICN-1040

Message `<timestamp>, [FICN-1040], <sequence-number>,, ERROR, <system-name>, HostTapeEgr:Tape:CmdReject Sense Data Rcvd:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>LastCmds=0x<Last 4 commands received from the channel for this device> SenseData:Bytes0-0xB=0x<Bytes 0-3 of sense data from the device> <Bytes 4-7 of sense data from the device> <Bytes 8-0x0b of sense data from the device>.`

Probable Cause Indicates an active disk emulation device received a FICON Purge Path from the channel.

Recommended Action If there was an unexpected job failure or IO Error associated with this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1041

Message `<timestamp>, [FICN-1041], <sequence-number>,, ERROR, <system-name>, HostTapeEgr:AS Link Level Reject (LRJ) from CU Rx Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>LastCmd=0x<Last 4 commands issued to this device from the channel> LastStatus=0x<Last 4 status values sent to the channel from this device>.`

Probable Cause Indicates an LRJ received from a device indicates that the CU has lost the logical path to the LPAR.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1042

Message

```
<timestamp>, [FICN-1042], <sequence-number>,, WARNING, <system-name>,
HostTapeIng:FICON Cancel received Path=<VEPortNumber HostDomain HostPort
DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>state=0x<the current emulation
state for this device>.
```

Probable Cause Indicates a job was cancelled during a write pipelining.

Recommended Action If this was an unexpected event (cancel is normally an operator event), contact your vendor's customer support for assistance.

Severity WARNING

FICN-1043

Message

```
<timestamp>, [FICN-1043], <sequence-number>,, ERROR, <system-name>,
HostTapeIng::FICON Selective Reset:Path=<VEPortNumber HostDomain HostPort
DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>state=0x<the current emulation
state for this device> LastCmds=0x<the last 4 commands received from the channel
for this device> LastStatus=0x<the last 4 status values presented to the channel
for this device>.
```

Probable Cause Indicates that protocol errors in emulation in the CU or network errors can cause a Selective Reset.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1044

Message

```
<timestamp>, [FICN-1044], <sequence-number>,, ERROR, <system-name>,
HostTapeIng:FICON Selective Reset:Path=<VEPortNumber HostDomain HostPort
DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>Elapsed Time=<the number of
seconds since the last IO started for this device>.<the number of milliseconds
since the last IO started for this device> seconds.
```

Probable Cause Indicates that protocol errors in emulation in the CU or network errors can cause Selective Reset.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1045

Message `<timestamp>, [FICN-1045], <sequence-number>,, WARNING, <system-name>, HostTapeIng:FICON Purge received:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates a purge path was received from the locally connected FICON channel. This is performed during the path recovery.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

Severity WARNING

FICN-1046

Message `<timestamp>, [FICN-1046], <sequence-number>,, WARNING, <system-name>, HostTapeIng:LRJ received on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>lastCmds=0x<Last 4 commands received from the channel for this device> lastStatus=0x<Last 4 status values presented to the channel for this device> treating as system reset event.`

Probable Cause Indicates an LRJ from a FICON channel indicates that the channel believes that it no longer has a path established to the CU.

Recommended Action This is normally an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1047

Message `<timestamp>, [FICN-1047], <sequence-number>,, ERROR, <system-name>, fcFicSetEmulation:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>FDCB Not Idle state=0x<Current emulation state of the FICON device> prevState=0x<Previous emulation state of the FICON device> set to state=0x<The new state to which the device is transitioning>.`

Probable Cause Indicates there is an internal emulation error. This message should not be encountered.

Recommended Action This is an unexpected event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1048

Message `<timestamp>, [FICN-1048], <sequence-number>,, WARNING, <system-name>, DevDiskEgr:FICON Cancel received Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> state=0x<Current emulation state of the FICON device> sflags=0x<The current emulation status flags>.`

Probable Cause Indicates the operator has cancelled a read or write job.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

Severity WARNING

FICN-1049

Message `<timestamp>, [FICN-1049], <sequence-number>,, WARNING, <system-name>, ProcessIngTirData:Lost Logical Path for Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> <CUADDR>Index=<Current processing index in the TIR data from the locally connected channel or control unit>.`

Probable Cause Indicates a TIR received from a FICON end point indicates that it no longer has an established path to its peer.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

Severity WARNING

FICN-1050

Message `<timestamp>, [FICN-1050], <sequence-number>,, WARNING, <system-name>, ProcessEgrTirData:Lost Logical Path for Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> <CUADDR> Index=<Current processing index in the TIR data from the remotely connected channel or control unit>.`

Probable Cause Indicates a TIR received from a far side FICON end point indicates that it no longer has an established path to its peer.

Recommended Action This is an unexpected event; contact your vendor's customer support for assistance.

Severity WARNING

FICN-1051

Message `<timestamp>, [FICN-1051], <sequence-number>,, INFO, <system-name>, XRC Session Established: SessID=<SDM Assigned Session ID>, Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates a PSF command has been received to initiate an XRC session with the extended DASD device.

Recommended Action No action is required. This is a part of the XRC session establishment.

Severity INFO

FICN-1052

Message `<timestamp>, [FICN-1052], <sequence-number>,, INFO, <system-name>, XRC Session Terminated: SessID=<SDM Assigned Session ID>, Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates a PSF command has been received to break an XRC session with the extended DASD device.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

Severity INFO

FICN-1053

Message `<timestamp>, [FICN-1053], <sequence-number>,, INFO, <system-name>, XRC Withdraw From Session: SessID=<SDM Assigned Session ID>, Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates a PSF command has been received to withdraw from the XRC session with the extended DASD device.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

Severity INFO

FICN-1054

Message `<timestamp>, [FICN-1054], <sequence-number>,, WARNING, <system-name>, XRC Device Suspended: SessID=<SDM Assigned Session ID>, Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates a PSF command has been received to suspend an XRC session with the extended DASD device.

Recommended Action If this was an unexpected event, please contact your vendor's customer support for assistance.

Severity WARNING

FICN-1055

Message `<timestamp>, [FICN-1055], <sequence-number>,, WARNING, <system-name>, XRC All Devices Suspended: SessID=<SDM Assigned Session ID>, Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates a suspend all devices from XRC session PSF command has been received to break an XRC session with the extended DASD device.

Recommended Action If this was an unexpected event, contact your vendor's customer support for assistance.

Severity WARNING

FICN-1056

Message `<timestamp>, [FICN-1056], <sequence-number>,, ERROR, <system-name>, FICON Emulation Error Error Code=<The internal emulation error code value>, Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> LastStates=0x<The 4 oldest emulation states for this device><The prior emulation state for this device><The current emulation state for this device>.`

Probable Cause Indicates an internal coding error within emulation processing.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1057

Message `<timestamp>, [FICN-1057], <sequence-number>,, ERROR, <system-name>, Error return from frame generation processing for a FICON device: Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates an internal resource shortage caused an error such that an emulation frame could not be created and sent to a device.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1058

Message `<timestamp>, [FICN-1058], <sequence-number>,, ERROR, <system-name>, Error return from frame generation processing for a FICON control unit: Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates an internal resource shortage caused an error such that an emulation frame could not be created and sent to a Control Unit.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1059

Message `<timestamp>, [FICN-1059], <sequence-number>,, ERROR, <system-name>, Error return from frame generation for a FICON Image: Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR >.`

Probable Cause Indicates an internal resource shortage caused an error such that an emulation frame could not be created and sent to an LPAR.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1060

Message `<timestamp>, [FICN-1060], <sequence-number>,, ERROR, <system-name>, Error return from fcFwdPrcEgressFrame: Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates an internal resource shortage caused an error such that an emulation frame could not be created and sent to a device.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1061

Message `<timestamp>, [FICN-1061], <sequence-number>,, ERROR, <system-name>, Error return from fcFwdRemoveEmulHashEntry: Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates an internal issue has been encountered in the removal of an existing fast path hash table entry.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1062

Message `<timestamp>, [FICN-1062], <sequence-number>,, ERROR, <system-name>, Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:LastStates=0x<prior emulation state> <previous emulation state> <current emulation state>.`

Probable Cause Indicates an abort operation has been received from the local FC interface for an active emulation exchange.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1063

Message

```
<timestamp>, [FICN-1063], <sequence-number>,, ERROR, <system-name>, Egress
Abort:Oxid=0x<the OXID of the aborted exchange>:Path=<VEPortNumber HostDomain
HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:LastStates=0x<prior
emulation state> <previous emulation state> <current emulation state>.
```

Probable Cause Indicates an abort operation has been received from a peer FC interface for an active emulation exchange.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1064

Message

```
<timestamp>, [FICN-1064], <sequence-number>,, INFO, <system-name>, Ingress
Abort:Oxid=0x<the OXID of the aborted exchange>:Unknown Path on GEPort=<GEPort
Number> VEPort=<VEPortNumber> from SID=0x<Source Domain><Source Port> to
DID=0x<Destination Domain><Destination Port>.
```

Probable Cause Indicates an abort operation has been received from a local FC interface for an exchange.

Recommended Action If there were associated IO errors at the same time as this event, contact your vendor's customer support for assistance.

Severity INFO

FICN-1065

Message

```
<timestamp>, [FICN-1065], <sequence-number>,, INFO, <system-name>, Egress
Abort:Oxid=0x<the OXID of the aborted exchange>:Unknown Path on GEPort=<GEPort
Number> VEPort=<VEPortNumber> from SID=0x<Source Domain><Source Port> to
DID=0x<Destination Domain><Destination Port>.
```

Probable Cause Indicates an abort operation has been received from a peer FC interface for an exchange.

Recommended Action If there were associated IO errors at the same time as this event, contact your vendor's customer support for assistance.

Severity INFO

FICN-1066

Message `<timestamp>, [FICN-1066], <sequence-number>,, WARNING, <system-name>, MemAllocFailed for GEPort=<GE0 or GE1 Number> VEport=<VEPortNumber> could not create required structure.`

Probable Cause Indicates an internal resource limit has been encountered such that additional control block memory could not be allocated.

Recommended Action This is an unexpected event, either the maximum number of emulation devices are already in use or there is an internal memory leak, contact your vendor's customer support for assistance.

Severity WARNING

FICN-1067

Message `<timestamp>, [FICN-1067], <sequence-number>,, ERROR, <system-name>, Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Abort for CH=0x<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR>.`

Probable Cause Indicates an abort operation has been received from a local FC interface for an emulation CH exchange.

Recommended Action If there were associated IO errors at the same time as this event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1068

Message `<timestamp>, [FICN-1068], <sequence-number>,, ERROR, <system-name>, Ingress Abort:Oxid=0x<the OXID of the aborted exchange>:Abort for CU=0x<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR> <CUADDR>.`

Probable Cause Indicates an abort operation has been received from a local FC interface for an emulaton CU exchange.

Recommended Action If there were associated IO errors at the same time as this event, please contact your vendor's customer support for assistance.

Severity ERROR

FICN-1069

Message `<timestamp>, [FICN-1069], <sequence-number>,, ERROR, <system-name>, Emulation Configuration Error on TunnelId <Tunnel ID>.`

Probable Cause Indicates an error has been noted in the FICON configuration. Refer to the string for the nature of the configuration issue.

Recommended Action If resolution of the configuration issue cannot be completed, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1070

Message `<timestamp>, [FICN-1070], <sequence-number>,, INFO, <system-name>, DevTapeIngr:Exceptional Status rcvd on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> state=0x<current emulation state> status=0x<the exceptional status value>.`

Probable Cause Indicates the normal end of tape status (0x0D or 0x05) is received from the device or error status (including Unit Check 0x02) is received from an active emulation device.

Recommended Action The end of tape is a normal event during pipelining and not the unit check. If there are associated IO error messages with this event, please contact your vendor's customer support for assistance.

Severity INFO

FICN-1071

Message `<timestamp>, [FICN-1071], <sequence-number>,, INFO, <system-name>, HostTapeIngr:Tape Loaded on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates the tape IOs are processed from a locally connected LPAR, which indicates that a tape is loaded on a device.

Recommended Action No action is required.

Severity INFO

FICN-1072

Message `<timestamp>, [FICN-1072], <sequence-number>,, INFO, <system-name>, DevTapeEgr:Tape Loaded on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>.`

Probable Cause Indicates the tape IOs are processed from a locally connected LPAR, which indicates that a tape is loaded on a device.

Recommended Action No action is required.

Severity INFO

FICN-1073

Message `<timestamp>, [FICN-1073], <sequence-number>,, INFO, <system-name>, HostTapeIngr:Unloaded:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:states=0x<4 prior emulation states>:cmds=0x<last 4 commands received from the channel for this device>:status=0x<last 4 status values sent to the channel for this device>:flags=0x<tape report bit flags (0x80-Tape Loaded,0x40-WriteEmul,0x20-RdBlkEmul,0x10-RdCpEmul)>.`

Probable Cause Indicates a Rewind and Unload IO has been processed from a locally connected LPAR, which indicates that a tape should be unloaded on a device.

Recommended Action No action is required.

Severity INFO

FICN-1074

Message `<timestamp>, [FICN-1074], <sequence-number>,, INFO, <system-name>, HostTapeIngr:WriteReport:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host write commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated write megabytes processed while this tape was loaded>.`

Probable Cause Indicates a Rewind and Unload IO has been processed from a locally connected LPAR and write pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1075

Message `<timestamp>, [FICN-1075], <sequence-number>,, INFO, <system-name>, HostTapeIngr:ReadBlkReport:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host read commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated read megabytes processed while this tape was loaded>.`

Probable Cause Indicates a Rewind and Unload IO has been processed from a locally connected LPAR and Read Block pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1076

Message `<timestamp>, [FICN-1076], <sequence-number>,, INFO, <system-name>, HostTapeIngr:ReadCpReport:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host read commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated read megabytes processed while this tape was loaded>.`

Probable Cause Indicates a Rewind and Unload IO has been processed from a locally connected LPAR and Read Channel Program pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1077

Message `<timestamp>, [FICN-1077], <sequence-number>,, INFO, <system-name>, DevTapeEgr:Unloaded:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:states=0x<4 prior emulation states>:cmds=0x<last 4 commands received from the channel for this device>:status=0x<last 4 status values received from the channel for this device>:flags=0x<tape report bit flags(0x80-Tape Loaded,0x40-WriteEmul,0x20-RdBlkEmul,0x10-RdCpEmul)>.`

Probable Cause Indicates a Rewind and Unload IO has been processed from a remotely connected LPAR, which indicates that a tape should be unloaded on a device.

Recommended Action No action is required.

Severity INFO

FICN-1078

Message `<timestamp>, [FICN-1078], <sequence-number>,, INFO, <system-name>, DevTapeEgr:ReadBlkReport:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host write commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated write megabytes processed while this tape was loaded>`

Probable Cause Indicates a Rewind and Unload IO has been processed from a remotely connected LPAR and write pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1079

Message `<timestamp>, [FICN-1079], <sequence-number>,, INFO, <system-name>, DevTapeEgr:WriteReport:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host read commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated read Kilobytes processed while this tape was loaded>.`

Probable Cause Indicates a Rewind and Unload IO has been processed from a remotely connected LPAR and Read Block pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1080

Message `<timestamp>, [FICN-1080], <sequence-number>,, INFO, <system-name>, DevTapeEgr:ReadCpReport:Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr>:Emuls=0x<the number of idle state to non-idle state transitions while this tape was loaded>:Cmds=0x<the number of emulated host read commands processed while this tape was loaded>:Chains=0x<the number of emulated host chains processed while this tape was loaded>:MBytes=<the number of emulated read Kilobytes processed while this tape was loaded>.`

Probable Cause Indicates a Rewind and Unload IO has been processed from a remotely connected LPAR and Read Channel Program pipelining was performed on the currently loaded tape.

Recommended Action No action is required.

Severity INFO

FICN-1081

Message `<timestamp>, [FICN-1081], <sequence-number>,, WARNING, <system-name>, DevTapeIng:LRJ received on Path=<VEPortNumber HostDomain HostPort DeviceDomain> <DevicePort LPAR CUADDR DeviceAddr> lastCmds=0x<Last 4 commands received from the channel for this device> lastStatus=0x<Last 4 status values presented to the channel for this device> treating as system reset event.`

Probable Cause Indicates an LRJ from a FICON channel indicates that the channel does not have a path established to the CU.

Recommended Action This is normally an unexpected event, contact your vendor's customer support for assistance.

Severity WARNING

FICN-1082

Message `<timestamp>, [FICN-1082], <sequence-number>,, WARNING, <system-name>, EmulEls:CSWR_RSCN received on GEPort=<GEPortNumber> VEPort=<VEPortNumber> Domain=0x<Domain Port Host> Port=0x<Device Side>.`

Probable Cause Indicates an attached port which had a FICON emulated path established has logged out from the switch.

Recommended Action This may be an unexpected event, contact your vendor's customer support for assistance.

Severity WARNING

FICN-1083

Message `<timestamp>, [FICN-1083], <sequence-number>,, WARNING, <system-name>, EmulEls:SW_RSCN received on GEPort=<GEPortNumber> VEPort=<VEPortNumber> Domain=0x<Domain Port Host> Port=0x<Device Side>.`

Probable Cause Indicates an attached port with the established FICON emulated path has logged out from the switch.

Recommended Action This may be an unexpected event, contact your vendor's customer support for assistance.

Severity WARNING

FICN-1084

Message `<timestamp>, [FICN-1084], <sequence-number>,, ERROR, <system-name>, fcFicInit: No DRAM2 memory available, FICON emulation is disabled.`

Probable Cause Indicates a faulty DRAM2 was detected and access to its address range is prohibited.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

FICN-1085

Message `<timestamp>, [FICN-1085], <sequence-number>,, INFO, <system-name>, FICON FCIP Tunnel is Up on GE<Either GE0 or GE1>,tunnel Id=<The configured tunnel ID (0-7)>.`

Probable Cause Indicates a FICON FCIP tunnel has been established successfully to the peer switch.

Recommended Action No action is required.

Severity INFO

FICN-1086

Message `<timestamp>, [FICN-1086], <sequence-number>,, ERROR, <system-name>, FICON FCIP Tunnel is Down on GE<Either GE0 or GE1>,tunnel Id=<The configured tunnel ID (0-7)>.`

Probable Cause Indicates a FICON FCIP tunnel to the peer switch has been terminated.

Recommended Action This is an unexpected event, contact your vendor's customer support for assistance.

Severity ERROR

Chapter

FICU System Messages

36

FICU-1001

Message `<timestamp>, [FICU-1001], <sequence-number>,, ERROR, <system-name>, <function name>: config<config Set(key)|Get(key)| Save> failed rc = <error>.`

Probable Cause Indicates that one of the configuration management functions failed. The *key* variable is a part of the Fabric OS configuration database and is for support use only. The *error* variable is an internal error number.

Recommended Action Execute an **haFailover** command on the switch if it has redundant control processors (CPs) or restart the switch. Run the **supportSave** command to check if your flash is full. If the flash is full, run the **supportSave** command to clear the core files. Refer to the *Fabric OS Command Reference Manual* for more information on these commands.

Severity ERROR

FICU-1002

Message `<timestamp>, [FICU-1002], <sequence-number>,, ERROR, <system-name>, <function name>: Failed to get RNID from Management Server: Domain=<domain>, rc=<error>.`

Probable Cause Indicates that the fibre connectivity control unit port (FICON-CUP) daemon failed to get the switch request node ID (RNID) from the management server because of a Fabric OS problem. The domain variable displays the domain ID of the target switch for this RNID. The error variable is an internal error number.

Recommended Action If this is a bladed switch, execute the **haFailover** command. If the problem persists, or if this is a nonbladed switch, download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on these commands.

Severity ERROR

FICU-1003

Message `<timestamp>, [FICU-1003], <sequence-number>,, WARNING, <system-name>, <function name>: <message> FICON-CUP License Not Installed: (<error>).`

Probable Cause Indicates that the fibre connectivity control unit port (FICON-CUP) license is not installed on the switch.

Recommended Action Run the **licenseShow** command to check the installed licenses on the switch. The switch cannot be managed using FICON-CUP commands until the FICON-CUP license is installed. Contact your switch supplier for a FICON-CUP license. Run the **licenseAdd** command to add the license to your switch.

Severity WARNING

FICU-1004

Message `<timestamp>, [FICU-1004], <sequence-number>,, WARNING, <system-name>, <function name>: Failed to set fabric manager server (FMS) mode: conflicting PID Format:<pid_format>, FMS Mode:<mode>.`

Probable Cause Indicates that a process ID (PID) format conflict was encountered. The core PID format is required for fibre connectivity control unit port (FICON-CUP).

The *pid_format* variable displays the PID format currently running on the fabric, and is one of the following:

- 0 is VC-encoded PID format
- 1 is core PID format
- 2 is extended-edge PID format

FMS mode displays whether fibre connectivity (FICON) Management Server mode is enabled; a 0 means this mode is enabled and a 1 means this mode is disabled.

Recommended Action For FICON Management Server mode (**fmsMode**) to be enabled, the core PID format must be used in the fabric. Change the PID format to core PID using the **configure** command and re-enable fmsMode using the **ficonCupSet** command. Refer to the *Fabric OS Administrator's Guide* for information on core PID mode and the *Fabric OS Command Reference Manual* for information on these commands.

Severity WARNING

FICU-1005

Message `<timestamp>, [FICU-1005], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module>, rc = <error>.`

Probable Cause Indicates that the initialization of a module within the fibre connectivity control unit port (FICON-CUP) daemon failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

FICU-1006

Message `<timestamp>, [FICU-1006], <sequence-number>,, WARNING, <system-name>, Control Device Allegiance Reset: (Logical Path: 0x<PID>:0x<channel image ID>)`

Probable Cause Indicates that the path with the specified PID and channel image ID lost allegiance to a fibre connectivity control unit port (FICON-CUP) device.

Recommended Action Check if the FICON channel corresponding to the PID in the message is functioning correctly.

Severity WARNING

FICU-1007

Message `<timestamp>, [FICU-1007], <sequence-number>,, WARNING, <system-name>, <function name>: Failed to allocate memory while performing <message>.`

Probable Cause Indicates that memory resources are low. This might be a transient problem.

Recommended Action If the message persists, check the memory usage on the switch, using the **memShow** command.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FICU-1008

Message `<timestamp>, [FICU-1008], <sequence-number>,, WARNING, <system-name>, FMS mode has been enabled. Ports:<port numbers> have been disabled due to port address conflict.`

Probable Cause Indicates that the specified ports were disabled when Fibre Connectivity (FICON) Management Server mode (**fmsMode**) was enabled. This is due to a port address conflict or the port address being reserved for the CUP management port.

Recommended Action No action is required.

Severity WARNING

FICU-1009

Message `<timestamp>, [FICU-1009], <sequence-number>,, WARNING, <system-name>, FMS Mode enable failed due to insufficient frame filtering resources on some ports.`

Probable Cause Indicates that the frame filtering resources required to enable Fibre Connectivity (FICON) Management Server mode (**fmsMode**) were not available on some of the ports.

Recommended Action Use the **perfDelFilterMonitor** command to delete the filter-based performance monitors used on all ports to free up the resources.

Severity WARNING

FICU-1010

Message `<timestamp>, [FICU-1010], <sequence-number>,, WARNING, <system-name>, FMS Mode enable failed due to address conflict with port <port number>.`

Probable Cause Indicates that the Fibre Connectivity (FICON) Management Server mode (**fmsMode**) was not enabled because the specified port which has an address conflict with the CUP management port is in use.

Recommended Action Use the **portDisable** command to disable the specified port to avoid the port address conflict.

Severity WARNING

FICU-1011

Message `<timestamp>, [FICU-1011], <sequence-number>,, INFO, <system-name>, FMS mode has been enabled.`

Probable Cause Indicates that the Fibre Connectivity (FICON) Management Server mode has been enabled.

Recommended Action No action is required.

Severity INFO

FICU-1012

Message `<timestamp>, [FICU-1012], <sequence-number>,, INFO, <system-name>, FMS mode has been disabled.`

Probable Cause Indicates that the Fibre Connectivity (FICON) Management Server mode has been disabled.

Recommended Action No action is required.

Severity INFO

FICU-1013

Message `<timestamp>, [FICU-1013], <sequence-number>,, WARNING, <system-name>, Host data file cannot be resetted to proper size.`

Probable Cause Indicates that the file system is too full to create a host data file of the proper size.

Recommended Action Create additional room in the file system and initiate a warm recovery.

Severity WARNING

FICU-1014

Message `<timestamp>, [FICU-1014], <sequence-number>,, INFO, <system-name>, CUP SBTOV Timeout - %s, Type(%s).`

Probable Cause Indicates that the FICON Host failed to send an IU within the SBTOV.

Recommended Action No Action is required.

Severity INFO

FICU-1015

Message `<timestamp>, [FICU-1015], <sequence-number>,, INFO, <system-name>, CUP SB Recovery DIB - %s, DIB_Type(%s).`

Probable Cause Indicates that the recovery DIB has been received.

Recommended Action No Action is required.

Severity INFO

FICU-1016

Message `<timestamp>, [FICU-1016], <sequence-number>,, INFO, <system-name>, CUP Exchange Abort - PortIdx(%02X), PortAddr(%02X), XID(%02X).`

Probable Cause Indicates that the CUP Exchange Abort was received.

Recommended Action No Action is required.

Severity INFO

FICU-1017

Message `<timestamp>, [FICU-1017], <sequence-number>,, WARNING, <system-name>, FMSMODE enable failed because reserved area is bound to a device.`

Probable Cause Indicates one or both of the reserved areas 0xFE and 0xFF is bound to a device.

Recommended Action Issue **wwnaddress –show** command to see all the devices currently bound to areas. Use **wwnaddress –unbind [WWN]** command to release the reserved area from the device.

Severity WARNING

FICU-1018

Message `<timestamp>, [FICU-1018], <sequence-number>,, WARNING, <system-name>, FMSMODE enable noticed swapped ports.`

Probable Cause Indicates some ports are swapped at the time of FMS Mode enable.

Recommended Action Verify expected FICON Port Address / Port Number relationship.

Severity WARNING

FICU-1019

Message `<timestamp>, [FICU-1019], <sequence-number>,, INFO, <system-name>, Switch has been set offline by LP(%s).`

Probable Cause Indicates the Fibre Connectivity (FICON) Management server has disabled switch.

Recommended Action No action is required.

Severity INFO

FICU-1020

Message `<timestamp>, [FICU-1020], <sequence-number>,, INFO, <system-name>, Port Addrs (%s) have been Blocked by %s.`

Probable Cause Indicates the Fibre Connectivity (FICON) Management server has blocked ports.

Recommended Action No action is required.

Severity INFO

FICU-1021

Message `<timestamp>, [FICU-1021], <sequence-number>,, INFO, <system-name>, Port Addrs (%s) have been UnBlocked by %s.`

Probable Cause Indicates the Fibre Connectivity (FICON) Management server has unblocked ports.

Recommended Action No action is required.

Severity INFO

FICU-1022

Message `<timestamp>, [FICU-1022], <sequence-number>,, ERROR, <system-name>, Detected FC8-48 and/or FC8-64 that are not manageable when FMS mode is enabled.`

Probable Cause Indicates presence of unmanageable ports such as 48 port blade ports in Virtual Fabric disabled chassis.

Recommended Action No action is required.

Severity ERROR

Chapter

FKLB System Messages

37

FKLB-1001

Message `<timestamp>, [FKLB-1001], <sequence-number>,, WARNING, <system-name>, exchange <xid> overlapped, pid=<pid>`

Probable Cause Indicates that the FC kernel driver has timed out the exchange while the application is still active. When the FC kernel driver reuses the exchange, the application will overlap. This happens on a timed-out exchange; it automatically recovers after the application times the exchange out.

Recommended Action No action is required.

Severity WARNING

Chapter

FLOD System Messages

38

FLOD-1001

Message `<timestamp>, [FLOD-1001], <sequence-number>, FFDC, WARNING, <system-name>, Unknown LSR type: port <port number>, type <LSR header type>`

Probable Cause Indicates that the link state record (LSR) type is unknown. The following two LSR header types are the only known types: 1 - Unicast and 3 - Multicast.

Recommended Action No action is required because the record is discarded.

Severity WARNING

FLOD-1003

Message `<timestamp>, [FLOD-1003], <sequence-number>,, WARNING, <system-name>, Link count exceeded in received LSR, value = <link count number>`

Probable Cause Indicates that the acceptable link count has exceeded in the received link state record (LSR).

Recommended Action No action is required because the record is discarded.

Severity WARNING

FLOD-1004

Message `<timestamp>, [FLOD-1004], <sequence-number>, FFDC, ERROR, <system-name>, Excessive LSU length = <LSU length>`

Probable Cause Indicates that the LSU size exceeds what the system can support.

Recommended Action Reduce the number of switches in the fabric or reduce the number of redundant ISLs between two switches.

Severity ERROR

FLOD-1005

Message `<timestamp>, [FLOD-1005], <sequence-number>,, WARNING, <system-name>, Invalid received domain ID: <domain number>`

Probable Cause Indicates that the received LSR contained an invalid domain number.

Recommended Action No action is required because the LSR is discarded.

Severity WARNING

FLOD-1006

Message
```
<timestamp>, [FLOD-1006], <sequence-number>,, WARNING, <system-name>,
Transmitting invalid domain ID: <domain number>
```

Probable Cause Indicates that the transmit LSR contained an invalid domain number.

Recommended Action No action is required because the LSR is discarded.

Severity WARNING

Chapter

FSPF System Messages

39

FSPF-1001

Message `<timestamp>, [FSPF-1001], <sequence-number>,, ERROR, <system-name>, Input Port <port number> out of range`

Probable Cause Indicates that the specified input port number is out of range; it does not exist on the switch.

Recommended Action No action is required.

Severity ERROR

FSPF-1002

Message `<timestamp>, [FSPF-1002], <sequence-number>,, INFO, <system-name>, Wrong neighbor ID (<domain ID>) in Hello message from port <port number>, expected ID = <domain ID>`

Probable Cause Indicates that the switch has received the wrong domain ID from a neighbor (adjacent) switch in the HELLO message from a specified port. This might happen when a domain ID for a switch has been changed.

Recommended Action No action is required.

Severity INFO

FSPF-1003

Message `<timestamp>, [FSPF-1003], <sequence-number>,, ERROR, <system-name>, Remote Domain ID <domain number> out of range, input port = <port number>`

Probable Cause Indicates that the specified remote domain ID is out of range.

Recommended Action No action is required because the frame is discarded.

Severity ERROR

FSPF-1005

Message `<timestamp>, [FSPF-1005], <sequence-number>,, ERROR, <system-name>, Wrong Section Id <section number>, should be <section number>, input port = <port number>`

Probable Cause Indicates that an incorrect section ID was reported from the specified input port. The section ID is used to identify a set of switches that share an identical topology database. The section ID is implemented inside the protocol. The error message itself will indicate the mismatched section ID. It should be set to 0 for a non-hierarchical fabric. Brocade switches support only section ID 0.

Recommended Action Use a frame analyzer to verify that the reported section ID is 0. Any connected switch from another manufacturer with a section ID other than 0 is incompatible in a fabric of SilkWorm switches. Disconnect the offending switch.

Severity ERROR

FSPF-1006

Message `<timestamp>, [FSPF-1006], <sequence-number>,, ERROR, <system-name>, FSPF Version <FSFP version> not supported, input port = <port number>`

Probable Cause Indicates that the FSPF version is not supported on the specified input port.

Recommended Action Update the FSPF version by running the **firmwareDownload** command to update the firmware to the latest version. All current versions of the Fabric OS support FSPF version 2.

Severity ERROR

FSPF-1007

Message `<timestamp>, [FSPF-1007], <sequence-number>,, ERROR, <system-name>, ICL triangular topology is broken between the neighboring domains: <domain number> and <domain number>. Please fix it ASAP.`

Probable Cause Indicates that the ICL triangular topology is broken and becomes linear. It may cause the frame drop or performance slowdown.

Recommended Action Connect the two domains using ICL or regular ISL to form a triangular topology.

Severity ERROR

FSPF-1008

Message `<timestamp>, [FSPF-1008], <sequence-number>,, INFO, <system-name>, ICL triangular topology is formed among the domains: <domain number> (self), <domain number> and <domain number>.`

Probable Cause Indicates that the ICL triangular topology is formed.

Recommended Action No action is required.

Severity INFO

Chapter

FSS System Messages

40

FSS-1001

Message `<timestamp>, [FSS-1001], <sequence-number>, SLOT cp-slot-number | CHASSIS, WARNING, <system-name>, Component (<component name>) dropping HA data update (<update ID>).`

Probable Cause Indicates that an application has dropped a high availability (HA) data update.

Recommended Action Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run the **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FSS-1002

Message `<timestamp>, [FSS-1002], <sequence-number>, SLOT cp-slot-number | CHASSIS, WARNING, <system-name>, Component (<component name>) sending too many concurrent HA data update transactions (<dropped update transaction ID>)`

Probable Cause Indicates that an application has sent too many concurrent high availability (HA) data updates.

Recommended Action Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run the **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FSS-1003

Message `<timestamp>, [FSS-1003], <sequence-number>, SLOT cp-slot-number | CHASSIS, WARNING, <system-name>, Component (<component name>) misused the update transaction (<transaction ID>) without marking the transaction beginning.`

Probable Cause Indicates that the Fabric OS state synchronization (FSS) service has dropped the update because an application has not set the transaction flag correctly.

Recommended Action Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run the **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FSS-1004

Message `<timestamp>, [FSS-1004], <sequence-number>, SLOT cp-slot-number | CHASSIS, ERROR, <system-name>, Memory shortage`

Probable Cause Indicates that the system ran out of memory.

Recommended Action Run the **memShow** command to view memory usage.

Run the **haSyncStart** command if this is a dual-CP system, or reboot the switch if it is a nonbladed system.

If the message persists, run the **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

FSS-1005

Message `<timestamp>, [FSS-1005], <sequence-number>, SLOT cp-slot-number | CHASSIS, WARNING, <system-name>, FSS read failure`

Probable Cause Indicates that the read system call to the Fabric OS state synchronization (FSS) device failed.

Recommended Action If the message persists, run the **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FSS-1006

Message `<timestamp>, [FSS-1006], <sequence-number>, SLOT cp-slot-number | CHASSIS, WARNING, <system-name>, No FSS message available`

Probable Cause Indicates that data is not available on the Fabric OS state synchronization (FSS) device.

Recommended Action If the message persists, run the **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FSS-1007

Message `<timestamp>, [FSS-1007], <sequence-number>, SLOT cp-slot-number | CHASSIS, CRITICAL, <system-name>, <component name>: Faulty Ethernet connection.`

Probable Cause Indicates that the Ethernet connection between the active control processor (CP) and standby CP is not healthy. The error occurs when the standby CP does not respond to a request from the active CP within five seconds. This usually indicates a problem with the internal Ethernet connection and a disruption of the synchronization process.

Recommended Action Check the Ethernet connection between the active CP and standby CP (interface eth1) by issuing net commands such as **ifconfig eth1** (as root) or run **supportShow/supportSave** to validate the network configuration; then try to restore the synchronization by issuing the **haSyncStart** command. If the problem persists, contact your switch service provider.

Severity CRITICAL

FSS-1008

Message

```
<timestamp>, [FSS-1008], <sequence-number>, SLOT cp-slot-number | CHASSIS,
CRITICAL, <system-name>, FSS Error: <Error Message>.
```

Probable Cause Indicates that an error has occurred.

Recommended Action Run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

FSS-1009

Message

```
<timestamp>, [FSS-1009], <sequence-number>, SLOT cp-slot-number | CHASSIS, ERROR,
<system-name>, FSS Error: <Error Message>.
```

Probable Cause Indicates that an error has occurred.

Recommended Action Run the **supportSave** command and contact your switch service provider.

Severity ERROR

FSS-1010

Message

```
<timestamp>, [FSS-1010], <sequence-number>, SLOT cp-slot-number | CHASSIS,
WARNING, <system-name>, FSS Warning: <Warning Message>.
```

Probable Cause Indicates that an error might have occurred.

Recommended Action No action is required.

Severity WARNING

FSS-1011

Message `<timestamp>, [FSS-1011], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, FSS Info: <Info Message>.`

Probable Cause Indicates an informational message only.

Recommended Action No action is required.

Severity INFO

Chapter

FSSM System Messages

41

FSSM-1002

Message `<timestamp>, [FSSM-1002], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, HA State is in sync.`

Probable Cause Indicates that the high availability (HA) state for the active control processor (CP) is in synchronization with the HA state of the standby CP. If the standby CP is healthy, then a failover is nondisruptive. For more information on the **haFailover** command, refer to the *Fabric OS Command Reference Manual*.

Recommended Action No action is required.

Severity INFO

FSSM-1003

Message `<timestamp>, [FSSM-1003], <sequence-number>, SLOT cp-slot-number | CHASSIS, WARNING, <system-name>, HA State out of sync.`

Probable Cause Indicates that the high availability (HA) state for the active control processor (CP) is out of synchronization with the HA state of the standby CP. If the active CP failover occurs when the HA state is out of sync, the failover is disruptive.

Recommended Action If this message was logged as a result of a user-initiated action (such as running the **Reboot** command), then no action is required.

Otherwise, issue the **haSyncStart** command on the active CP and try resynchronizing the HA state. If the HA state does not become synchronized, run the **haDump** command to diagnose the problem.

If the problem persists, run the **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

FSSM-1004

Message `<timestamp>, [FSSM-1004], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, Incompatible software version in HA synchronization.`

Probable Cause Indicates that the active control processor (CP) and the standby CP in a dual CP system are running firmware that are incompatible with each other. If the active CP fails, the failover will be disruptive. In a switch system, this message is logged when a firmware upgrade or downgrade was invoked. The new firmware version is not compatiable with the current running version. This causes a disruptive firmware upgrade or downgrade.

Recommended Action For a dual CP system, run the **firmwareDownload** command to load compatible firmware on the standby CP. For details on this command, refer to the *Fabric OS Command Reference Manual*.

Severity INFO

Chapter

FW System Messages

42

FW-1001

Message `<timestamp>, [FW-1001], <sequence-number>,, INFO, <system-name>, <label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the internal temperature of the switch has changed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. To prevent recurring messages, disable the changed alarm for this threshold.

Severity INFO

FW-1002

Message `<timestamp>, [FW-1002], <sequence-number>,, WARNING, <system-name>, <Label>, is below low boundary (High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the internal temperature of the switch has fallen below the low boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Typically, low temperatures means that the fans and airflow of a switch are functioning normally.

Verify that the location temperature is within the operational range of the switch. Refer to the hardware reference manual for the environmental temperature range of your switch.

Severity WARNING

FW-1003

Message `<timestamp>, [FW-1003], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the internal temperature of the switch has risen above the high boundary to a value that might damage the switch.

Recommended Action This message generally appears when a fan fails. If so, a fan failure message accompanies this message. Replace the fan field-replaceable unit (FRU).

Severity WARNING

FW-1004

Message `<timestamp>, [FW-1004], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the internal temperature of the switch has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1009

Message `<timestamp>, [FW-1009], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the state of the power supply has changed from faulty to functional, or from functional to faulty.

Recommended Action If the power supply is functioning correctly, no action is required.

If the power supply is functioning below the acceptable boundary, verify that it is seated correctly in the chassis. Run the **psShow** command to view the status of the power supply. If the power supply continues to be a problem, replace the faulty power supply.

Severity INFO

FW-1010

Message `<timestamp>, [FW-1010], <sequence-number>,, WARNING, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the power supply is faulty. The power supply is not producing enough power.

Recommended Action Verify that you have installed the power supply correctly and that it is correctly seated in the chassis. If the problem persists, replace the faulty power supply.

Severity WARNING

FW-1011

Message `<timestamp>, [FW-1011], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the power supply is functioning properly.

Recommended Action Set the high boundary above the normal operation range.

Severity INFO

FW-1012

Message `<timestamp>, [FW-1012], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the power supply counter changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1033

Message `<timestamp>, [FW-1033], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the temperature of the small form-factor pluggable (SFP) has changed. Frequent fluctuations in SFP temperature might indicate a deteriorating SFP.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1034

Message `<timestamp>, [FW-1034], <sequence-number>,, WARNING, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the temperature of the small form-factor pluggable (SFP) has fallen below the low boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity WARNING

FW-1035

Message `<timestamp>, [FW-1035], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the temperature of the small form-factor pluggable (SFP) has risen above the high boundary. Frequent fluctuations in temperature might indicate a deteriorating SFP.

Recommended Action Replace the SFP.

Severity WARNING

FW-1036

Message `<timestamp>, [FW-1036], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the temperature of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. Frequent fluctuations in temperature might indicate a deteriorating SFP.

Recommended Action No action is required.

Severity INFO

FW-1037

Message `<timestamp>, [FW-1037], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the receive power value of the small form-factor pluggable (SFP) has changed. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action Incoming laser fluctuations usually indicate a deteriorating SFP. If this message occurs repeatedly, replace the SFP.

Severity INFO

FW-1038

Message `<timestamp>, [FW-1038], <sequence-number>,, WARNING, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the receive power value of the small form-factor pluggable (SFP) has fallen below the low boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity WARNING

FW-1039

Message

```
<timestamp>, [FW-1039], <sequence-number>,, WARNING, <system-name>, <Label>, is
above high boundary(High=<High value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable Cause Indicates that the receive power value of the small form-factor pluggable (SFP) has risen above the high boundary. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action Replace the SFP before it deteriorates.

Severity WARNING

FW-1040

Message

```
<timestamp>, [FW-1040], <sequence-number>,, INFO, <system-name>, <Label>, is
between high and low boundaries(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the receive power value of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. The receive performance area measures the amount of incoming laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1041

Message

```
<timestamp>, [FW-1041], <sequence-number>,, INFO, <system-name>, <Label>, value
has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has changed. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action Transmitting laser fluctuations usually indicate a deteriorating SFP. If this message occurs repeatedly, replace the SFP.

Severity INFO

FW-1042

Message

```
<timestamp>, [FW-1042], <sequence-number>,, WARNING, <system-name>, <Label>, is
below low boundary(High=<High value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable Cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has fallen below the low boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity WARNING

FW-1043

Message

```
<timestamp>, [FW-1043], <sequence-number>,, WARNING, <system-name>, <Label>, is
above high boundary(High=<High value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable Cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has risen above the high boundary. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action Replace the SFP.

Severity WARNING

FW-1044

Message

```
<timestamp>, [FW-1044], <sequence-number>,, INFO, <system-name>, <Label>, is
between high and low boundaries(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the transmit power value of the small form-factor pluggable (SFP) has changed from a value outside of the acceptable range to a value within the acceptable range. The transmit performance area measures the amount of outgoing laser to help you determine if the SFP is in good working condition or not. If the counter often exceeds the threshold, the SFP is deteriorating.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1045

Message `<timestamp>, [FW-1045], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed. If the supplied voltage of the SFP transceiver is outside of the normal range, this might indicate a hardware failure.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent messages indicate that you must replace the SFP.

Severity INFO

FW-1046

Message `<timestamp>, [FW-1046], <sequence-number>,, WARNING, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has fallen below the low boundary.

Recommended Action Verify that your optical components are clean and function properly. Replace deteriorating cables or SFPs. Check for damage from heat or age.

Severity WARNING

FW-1047

Message `<timestamp>, [FW-1047], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has risen above the high boundary.

Recommended Action The supplied current of the SFP transceiver is outside of the normal range, indicating possible hardware failure. If the current rises above the high boundary, you must replace the SFP.

Severity WARNING

FW-1048

Message `<timestamp>, [FW-1048], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1049

Message `<timestamp>, [FW-1049], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed.

Recommended Action Frequent voltage fluctuations are an indication that the SFP is deteriorating. Replace the SFP.

Severity INFO

FW-1050

Message `<timestamp>, [FW-1050], <sequence-number>,, WARNING, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has fallen below the low boundary.

Recommended Action Configure the low threshold to 1 so that the threshold triggers an alarm when the value falls to 0 (Out_of_Range). If continuous or repeated alarms occur, replace the SFP before it deteriorates.

Severity WARNING

FW-1051

Message `<timestamp>, [FW-1051], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has risen above the high boundary. High voltages indicate possible hardware failures.

Recommended Action Frequent voltage fluctuations are an indication that the SFP is deteriorating. Replace the SFP.

Severity WARNING

FW-1052

Message `<timestamp>, [FW-1052], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the value of the small form-factor pluggable (SFP) voltage has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1113

Message `<timestamp>, [FW-1113], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of times E_Ports have gone down has changed. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended Action Check both ends of the physical connection and verify that the SFPs and cables are functioning properly.

Severity INFO

FW-1114

Message `<timestamp>, [FW-1114], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of times E_Ports have gone down has fallen below the low boundary. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors. A low number of E_Port failures means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1115

Message `<timestamp>, [FW-1115], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of times E_Ports have gone down has risen above the high boundary. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Check both ends of the physical connection and verify that the SFP functions properly.

Severity INFO

FW-1116

Message `<timestamp>, [FW-1116], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of times E_Ports have gone down has changed from a value outside of the acceptable range to a value within the acceptable range. E_Ports go down each time you remove a cable or small form-factor pluggable (SFP). SFP failures also cause E_Ports to go down. E_Port downs might be caused by transient errors.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1117

Message `<timestamp>, [FW-1117], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of fabric reconfigurations has changed. The following actions can cause a fabric reconfiguration:

- two switches with the same domain ID have connected to one another.
- two fabrics have joined.
- an E_Port has gone offline.
- a principal link has segmented from the fabric.

Recommended Action Verify that the cable is properly connected at both ends. Verify that the small form-factor pluggables (SFPs) have not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

Severity INFO

FW-1118

Message `<timestamp>, [FW-1118], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of fabric reconfigurations has fallen below the low boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

A low number of fabric reconfigurations means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1119

Message `<timestamp>, [FW-1119], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of fabric reconfigurations has risen above the high boundary. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended Action Verify that all interswitch link (ISL) cables are properly connected at both ends. Verify that the small form-factor pluggable (SFP) has not become faulty. An inexplicable fabric reconfiguration might be a transient error and might not require troubleshooting.

Severity INFO

FW-1120

Message `<timestamp>, [FW-1120], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of fabric reconfigurations has changed from a value outside of the acceptable range to a value within the acceptable range. The following occurrences can cause a fabric reconfiguration:

- Two switches with the same domain ID have connected to one another.
- Two fabrics have joined.
- An E_Port has gone offline.
- A principal link has segmented from the fabric.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1121

Message `<timestamp>, [FW-1121], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of domain ID changes has changed. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1122

Message `<timestamp>, [FW-1122], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of domain ID changes has fallen below the low boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch. A low number of domain ID changes means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1123

Message `<timestamp>, [FW-1123], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of domain ID changes has risen above the high boundary. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1124

Message `<timestamp>, [FW-1124], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of domain ID changes has changed from a value outside of the acceptable range to a value within the acceptable range. Domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to the switch.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1125

Message `<timestamp>, [FW-1125], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of segmentations has changed. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1126

Message `<timestamp>, [FW-1126], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of segmentations has fallen below the low boundary. Segmentation changes might occur due to:

- Zone conflicts.

- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

A low number of segmentation errors means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1127

Message

```
<timestamp>, [FW-1127], <sequence-number>,, INFO, <system-name>, <Label>, is
above high boundary(High=<High value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable Cause Indicates that the number of segmentations has risen above the high boundary. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1128

Message

```
<timestamp>, [FW-1128], <sequence-number>,, INFO, <system-name>, <Label>, is
between high and low boundaries(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the number of segmentations has changed from a value outside of the acceptable range to a value within the acceptable range. Segmentation changes might occur due to:

- Zone conflicts.
- Domain conflicts.
- Segmentation of the principal link between two switches.
- Incompatible link parameters. During E_Port initialization, ports exchange link parameters. Rarely, incompatible parameters result in segmentation.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1129

Message `<timestamp>, [FW-1129], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of zone changes has changed. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1130

Message `<timestamp>, [FW-1130], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of zone changes has fallen below the low boundary. Zone changes occur when there is a change to the effective zone configuration. A low number of zone configuration changes means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1131

Message `<timestamp>, [FW-1131], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of zone changes has risen above the high boundary. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1132

Message `<timestamp>, [FW-1132], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of zone changes has changed from a value outside of the acceptable range to a value within the acceptable range. Zone changes occur when there is a change to the effective zone configuration.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1133

Message `<timestamp>, [FW-1133], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of fabric logins has changed. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1134

Message `<timestamp>, [FW-1134], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of fabric logins has fallen below the low boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI. A low number of fabric logins means that the fabric is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1135

Message `<timestamp>, [FW-1135], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of fabric logins has risen above the high boundary. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1136

Message `<timestamp>, [FW-1136], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of fabric logins has changed from a value outside of the acceptable range to a value within the acceptable range. Fabric logins occur when a port or device initializes with the fabric. The event is called a fabric login or FLOGI.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1137

Message `<timestamp>, [FW-1137], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of small form-factor pluggable (SFP) state changes has changed. SFP state changes occur when the SFP is inserted or removed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1138

Message `<timestamp>, [FW-1138], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of small form-factor pluggable (SFP) state changes has fallen below the low boundary. SFP state changes occur when the SFP is inserted or removed. A low number of SFP state changes means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1139

Message `<timestamp>, [FW-1139], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of small form-factor pluggable (SFP) state changes has risen above the high boundary. SFP state changes occur when the SFP is inserted or removed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1140

Message

```
<timestamp>, [FW-1140], <sequence-number>,, INFO, <system-name>, <Label>, is
between high and low boundaries(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the number of small form-factor pluggable (SFP) state changes has changed from a value outside of the acceptable range to a value within the acceptable range. SFP state changes occur when the SFP is inserted or removed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1160

Message

```
<timestamp>, [FW-1160], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Probable Cause Indicates that the number of link failures that the port experiences has changed. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Losses of synchronization commonly causes link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

Severity INFO

FW-1161

Message

```
<timestamp>, [FW-1161], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the number of link failures that the port experiences has fallen below the low boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them. A low number of link loss errors means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1162

Message

```
<timestamp>, [FW-1162], <sequence-number>,, WARNING, <system-name>, <Port Name>,
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the number of link failures that the port experiences has risen above the high boundary. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Losses of synchronization commonly cause link failures. If you receive concurrent loss of synchronization errors, troubleshoot the loss of synchronization.

Severity WARNING

FW-1163

Message

```
<timestamp>, [FW-1163], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of link failures that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1164

Message `<timestamp>, [FW-1164], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of synchronization losses that the port experiences has changed. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

If you continue to experience synchronization loss errors, troubleshoot your host bus adaptor (HBA) and contact your switch service provider.

Severity INFO

FW-1165

Message `<timestamp>, [FW-1165], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of synchronization losses that the port experiences has fallen below the low boundary. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of synchronization losses means that the switch is functioning normally.

Severity INFO

FW-1166

Message `<timestamp>, [FW-1166], <sequence-number>,, WARNING, <system-name>, <Port Name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of synchronization losses that the port experiences has risen above the high boundary. Loss-of-synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

If you continue to experience loss-of-synchronization errors, troubleshoot your host bus adaptor (HBA) and contact your switch service provider.

Severity WARNING

FW-1167

Message `<timestamp>, [FW-1167], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of synchronization losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1168

Message `<timestamp>, [FW-1168], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of signal losses that the port experiences has changed. Loss of signal generally indicates a physical problem.

Recommended Action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Severity INFO

FW-1169

Message `<timestamp>, [FW-1169], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of signal losses that the port experiences has fallen below the low boundary. Loss of signal generally indicates a physical problem.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of signal loss errors means that the switch is functioning normally.

Severity INFO

FW-1170

Message `<timestamp>, [FW-1170], <sequence-number>,, WARNING, <system-name>, <Port Name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of signal losses that the port experiences has risen above the high boundary. Loss of signal generally indicates a physical problem.

Recommended Action Check both ends of your cable connection. Verify that the cable is not faulty.

Severity WARNING

FW-1171

Message

```
<timestamp>, [FW-1171], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of signal losses that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Loss of signal generally indicates a physical problem.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent loss of signal generally indicates a physical problem.

Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Severity INFO

FW-1172

Message

```
<timestamp>, [FW-1172], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, value has changed(High=<High value>, Low=<Low value>). Current value is
<Value> <Unit>.
```

Probable Cause Indicates that the number of protocol errors that the port experiences has changed. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Severity INFO

FW-1173

Message

```
<timestamp>, [FW-1173], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the number of protocol errors that the port experiences has fallen below the low boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems. A low number of protocol errors means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1174

Message `<timestamp>, [FW-1174], <sequence-number>,, WARNING, <system-name>, <Port Name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of protocol errors that the port experiences has risen above the high boundary. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action Check both ends of your connection. Verify that your cable and small form-factor pluggable (SFP) are not faulty.

Severity WARNING

FW-1175

Message `<timestamp>, [FW-1175], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of protocol errors that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1176

Message `<timestamp>, [FW-1176], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid words that the port experiences has changed. Invalid words usually indicate a hardware problem with an small form-factor pluggable (SFP) or cable.

Recommended Action Check both ends of your connections, your SFP, and your cable to verify that none are faulty.

Severity INFO

FW-1177

Message `<timestamp>, [FW-1177], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid words that the port experiences has fallen below the low boundary. Invalid words usually indicate a hardware problem with an small form-factor pluggable (SFP) or cable. A low number of invalid words means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1178

Message `<timestamp>, [FW-1178], <sequence-number>,, WARNING, <system-name>, <Port Name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid words that the port experiences has risen above the high boundary. Invalid words usually indicate a hardware problem with an small form-factor pluggable (SFP) or cable.

Recommended Action Check both ends of your connections, your SFP, and your cable to verify that none are faulty.

Severity WARNING

FW-1179

Message `<timestamp>, [FW-1179], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid words that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Invalid words usually indicate a hardware problem with an small form-factor pluggable (SFP) or cable.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1180

Message `<timestamp>, [FW-1180], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has changed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity INFO

FW-1181

Message

```
<timestamp>, [FW-1181], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has fallen below the low boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of invalid CRCs means that the switch is functioning normally.

Severity INFO

FW-1182

Message

```
<timestamp>, [FW-1182], <sequence-number>,, WARNING, <system-name>, <Port Name>,
<Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value
is <Value> <Unit>.
```

Probable Cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has risen above the high boundary.

Recommended Action This error generally indicates an deteriorating fabric hardware. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity WARNING

FW-1183

Message

```
<timestamp>, [FW-1183], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, is between high and low boundaries(High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity INFO

FW-1184

Message `<timestamp>, [FW-1184], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has changed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1185

Message `<timestamp>, [FW-1185], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has fallen below the low boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1186

Message `<timestamp>, [FW-1186], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has risen above the high boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1187

Message `<timestamp>, [FW-1187], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1188

Message `<timestamp>, [FW-1188], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has changed.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1189

Message `<timestamp>, [FW-1189], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has fallen below the low boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1190

Message `<timestamp>, [FW-1190], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has risen above the high boundary.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1191

Message `<timestamp>, [FW-1191], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1192

Message `<timestamp>, [FW-1192], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of state changes that the port experiences has changed. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1193

Message `<timestamp>, [FW-1193], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of state changes that the port experiences has fallen below the low boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

A low number of port state changes means that the switch is functioning normally.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1194

Message `<timestamp>, [FW-1194], <sequence-number>,, WARNING, <system-name>, <Port Name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of state changes that the port experiences has risen above the high boundary. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity WARNING

FW-1195

Message `<timestamp>, [FW-1195], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of state changes that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1196

Message `<timestamp>, [FW-1196], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of link resets that the port experiences has changed. Link resets occur due to link timeout errors that indicate no frame activity at all.

Recommended Action Check both ends of your cable connection. Verify if the cable and small form-factor pluggables (SFPs) are faulty.

Severity INFO

FW-1197

Message `<timestamp>, [FW-1197], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of link resets that the port experiences has fallen below the low boundary. Link resets occur due to link timeout errors that indicate no frame activity at all.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation. A low number of link resets means that the switch is functioning normally.

Severity INFO

FW-1198

Message `<timestamp>, [FW-1198], <sequence-number>,, WARNING, <system-name>, <Port Name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of link resets that the port experiences has risen above the high boundary. Link resets occur due to link timeout errors that indicate no frame activity at all. Both physical and hardware problems can cause link resets to increase.

Recommended Action Check both ends of your cable connection. Verify if the cable and small form-factor pluggables (SFPs) are faulty.

Severity WARNING

FW-1199

Message `<timestamp>, [FW-1199], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is between high and low boundaries (High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of link resets that the port experiences has changed from a value outside of the acceptable range to a value within the acceptable range. Link resets occur due to link timeout errors that indicate no frame activity at all. Both physical and hardware problems can cause link resets to increase.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1200

Message `<timestamp>, [FW-1200], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of C3 transmit time out frames has changed.

Recommended Action Check the target device; it could be slow.

Severity INFO

FW-1201

Message

```
<timestamp>, [FW-1201], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, is below low boundaries (High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable Cause Indicates that the number of C3 transmit time out frames is below low threshold.

Recommended Action Respond to this message as it is appropriate to the particular policy of the end-user installation. A low number of C3 discard means that the switch is functioning normally.

Severity INFO

FW-1202

Message

```
<timestamp>, [FW-1202], <sequence-number>,, WARNING, <system-name>, <Port Name>,
<Label>, is above high boundaries (High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>.
```

Probable Cause Indicates that the number of C3 transmit time out frames is above high threshold.

Recommended Action Check the target device; it could be slow.

Severity WARNING

FW-1203

Message

```
<timestamp>, [FW-1203], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, is between high and low boundaries (High=<High value>, Low=<Low value>).
Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of C3 transmit time out frames is between high and low thresholds.

Recommended Action Check the target device; it could be slow.

Severity INFO

FW-1204

Message `<timestamp>, [FW-1204], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the trunk utilization has changed.

Recommended Action No action required.

Severity INFO

FW-1205

Message `<timestamp>, [FW-1205], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is below low boundaries (High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the trunk utilization has reduced.

Recommended Action No action required.

Severity INFO

FW-1206

Message `<timestamp>, [FW-1206], <sequence-number>,, WARNING, <system-name>, <Port Name>, <Label>, is between high and low boundaries (High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the trunk utilization has gone above its threshold level.

Recommended Action Increase the bandwidth by adding more links to the trunk.

Severity WARNING

FW-1207

Message `<timestamp>, [FW-1207], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, is between high and low boundaries (High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the trunk utilization is between low and high thresholds.

Recommended Action No action required.

Severity INFO

FW-1244

Message `<timestamp>, [FW-1244], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of end-to-end (EE) word frames that the switch receives has changed. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1245

Message `<timestamp>, [FW-1245], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of end-to-end (EE) word frames that the switch receives has fallen below the low boundary. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1246

Message `<timestamp>, [FW-1246], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of end-to-end (EE) word frames that the switch receives has risen above the high boundary. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1247

Message `<timestamp>, [FW-1247], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of end-to-end (EE) word frames that the switch receives has changed from a value outside of the acceptable range to a value within the acceptable range. Receive performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1248

Message `<timestamp>, [FW-1248], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of end-to-end (EE) word frames that the switch transmits has changed. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1249

Message `<timestamp>, [FW-1249], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of end-to-end (EE) word frames that the switch transmits has fallen below the low boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1250

Message `<timestamp>, [FW-1250], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of end-to-end (EE) word frames that the switch transmits has risen above the high boundary. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1251

Message `<timestamp>, [FW-1251], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of end-to-end (EE) word frames that the switch transmits has changed from a value outside of the acceptable range to a value within the acceptable range. Transmit performance messages appear due to the number of word frames that travel from the configured S_ID to the D_ID pair.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1272

Message `<timestamp>, [FW-1272], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of frame types or commands that the port receives has changed. The port has received small computer system interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1273

Message `<timestamp>, [FW-1273], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of frame types or commands that the port receives has fallen below the low boundary. The port has received a small computer system interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1274

Message `<timestamp>, [FW-1274], <sequence-number>,, INFO, <system-name>, <Label>, is above high boundary(High=<Filter Counter>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of frame types or commands that the port receives has risen above the high boundary. The port has received a small computer system interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1275

Message `<timestamp>, [FW-1275], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of frame types or commands that the port receives has changed from a value outside of the acceptable range to a value within the acceptable range. The port has received a small computer system interface (SCSI) Read, SCSI Write, SCSI Read and Write, SCSI Traffic, or IP commands in a frame.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1296

Message `<timestamp>, [FW-1296], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of Telnet violations has changed. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1297

Message `<timestamp>, [FW-1297], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of Telnet violations has fallen below the low boundary. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action No action is required.

Severity INFO

FW-1298

Message `<timestamp>, [FW-1298], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of Telnet violations has risen above the high boundary. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1299

Message `<timestamp>, [FW-1299], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of Telnet violations has changed from a value outside of the acceptable range to a value within the acceptable range. Telnet violations indicate that a Telnet connection request has been received from an unauthorized IP address. The TELNET_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish Telnet connections to switches in the fabric.

Recommended Action No action is required.

Severity INFO

FW-1300

Message `<timestamp>, [FW-1300], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of hypertext transfer protocol (HTTP) violations has changed. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended Action Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1301

Message `<timestamp>, [FW-1301], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of hypertext transfer protocol (HTTP) violations has fallen below the low boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended Action No action is required.

Severity INFO

FW-1302

Message `<timestamp>, [FW-1302], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of hypertext transfer protocol (HTTP) violations has risen above the high boundary. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended Action Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1303

Message `<timestamp>, [FW-1303], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of hypertext transfer protocol (HTTP) violations has changed from a value outside of the acceptable range to a value within the acceptable range. HTTP violations indicate that a browser connection request has been received from an unauthorized IP address. The HTTP_POLICY contains a list of internet protocol (IP) addresses that are authorized to establish browser connections to the switches in the fabric.

Recommended Action No action is required.

Severity INFO

FW-1308

Message `<timestamp>, [FW-1308], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of simple network management protocol read (RSNMP) violations has changed. RSNMP violations indicate that an SNMP “get” operation request has been received from an unauthorized IP address.

Recommended Action Run the **errShow** command to determine the IP address that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1332

Message `<timestamp>, [FW-1332], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of switch connection control policy (SCC) violations has changed. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by world wide name (WWN) that are allowed to be members of a fabric.

Recommended Action Run the **errShow** command to determine the WWN of the device that sent the request. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1333

Message `<timestamp>, [FW-1333], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of switch connection control policy (SCC) violations has fallen below the low boundary. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by world wide names (WWNs) that are allowed to be members of a fabric.

Recommended Action No action is required.

Severity INFO

FW-1335

Message `<timestamp>, [FW-1335], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of switch connection control policy (SCC) violations has changed from a value outside of the acceptable range to a value within the acceptable range. SCC violations indicate that an unauthorized switch tried to join the fabric. The SCC_POLICY contains a list of switches by world wide names (WWNs) that are allowed to be members of a fabric.

Recommended Action No action is required.

Severity INFO

FW-1336

Message `<timestamp>, [FW-1336], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of device cable connection (DCC) violations has changed. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically host bus adaptor (HBA) ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the world wide name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action Run the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1337

Message `<timestamp>, [FW-1337], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of device cable connection (DCC) violations has fallen below the low boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically host bus adaptor (HBA) ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request, the world wide name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action No action is required.

Severity INFO

FW-1338

Message `<timestamp>, [FW-1338], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of device cable connection (DCC) violations has risen above the high boundary. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically host bus adaptor (HBA) ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request that the world wide name ((WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action Run the **errShow** command to determine the device WWN, switch WWN, and switch port. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1339

Message `<timestamp>, [FW-1339], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of device cable connection (DCC) violations has changed from a value outside of the acceptable range to a value within the acceptable range. DCC violations indicate that an unauthorized device tried to join the fabric. The DCC_POLICY allows for the specification of rules for binding device ports (typically host bus adaptor (HBA) ports) to specific switch ports. DCC policies ensure that whenever a device performs a fabric login (FLOGI) request that the world wide name (WWN) specified in the FLOGI is validated to be connected to the authorized port. Enforcement for private loop devices not performing FLOGI is done through the name server.

Recommended Action No action is required.

Severity INFO

FW-1340

Message `<timestamp>, [FW-1340], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of login violations has changed. Login violations indicate that a login failure has been detected.

Recommended Action Run the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1341

Message `<timestamp>, [FW-1341], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of login violations has fallen below the low boundary. Login violations indicate that a login failure has been detected.

Recommended Action No action is required.

Severity INFO

FW-1342

Message `<timestamp>, [FW-1342], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of login violations has risen above the high boundary. Login violations indicate that a login failure has been detected.

Recommended Action Run the **errShow** command to determine the IP location of the login attempt. Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1343

Message `<timestamp>, [FW-1343], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of login violations has changed from a value outside of the acceptable range to a value within the acceptable range. Login violations indicate that a login failure has been detected.

Recommended Action No action is required.

Severity INFO

FW-1349

Message `<timestamp>, [FW-1349], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid signatures has fallen below the low boundary. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action No action is required.

Severity INFO

FW-1350

Message `<timestamp>, [FW-1350], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid signatures has risen above the high boundary. Invalid-signature violations indicate that a packet with an invalid signature has been received from the primary fabric configuration server (FCS). When the primary FCS downloads a new configuration to the other switches in the fabric, the packet is signed using the private key of the primary FCS. The receiving switch has to verify this signature with the public key of the primary FCS switch. If verification fails, it rejects the packet. This counter keeps track of the number of packets received with invalid signatures.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1352

Message

```
<timestamp>, [FW-1352], <sequence-number>,, INFO, <system-name>, <Label>, value
has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of invalid certificates has changed. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1353

Message

```
<timestamp>, [FW-1353], <sequence-number>,, INFO, <system-name>, <Label>, is
below low boundary(High=<High value>, Low=<Low value>). Current value is <Value>
<Unit>.
```

Probable Cause Indicates that the number of invalid certificates has fallen below the low boundary. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action No action is required.

Severity INFO

FW-1354

Message `<timestamp>, [FW-1354], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid certificates has risen above the high boundary. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1355

Message `<timestamp>, [FW-1355], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of invalid certificates has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates that a packet with an invalid certificate has been received from the primary fabric configuration server (FCS). Before a new primary FCS switch sends any configuration data to any switch in the fabric, it first sends its certificate to all the switches in the fabric. The receiving switch has to verify that the sender is the primary FCS switch and its certificate is signed by the Root CA recognized by the receiving switch. This counter keeps track of the number of packets received with invalid certificates.

Recommended Action No action is required.

Severity INFO

FW-1356

Message `<timestamp>, [FW-1356], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of authentication failures has changed. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly, or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1357

Message `<timestamp>, [FW-1357], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of authentication failures has fallen below the low boundary. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action No action is required.

Severity INFO

FW-1358

Message `<timestamp>, [FW-1358], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of authentication failures has risen above the high boundary. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1359

Message `<timestamp>, [FW-1359], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of authentication failures has changed from a value outside of the acceptable range to a value within the acceptable range. Authentication failures can occur for many reasons. The switch on the other side might not support the protocol, have an invalid certificate, not be signed properly or send unexpected packets. The port where authentication fails is segmented. This counter keeps track of the number of authentication failures.

Recommended Action No action is required.

Severity INFO

FW-1364

Message `<timestamp>, [FW-1364], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of time service (TS) out-of-sync violations has changed.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1365

Message `<timestamp>, [FW-1365], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of time service (TS) out-of-sync violations has fallen below the low boundary.

Recommended Action No action is required.

Severity INFO

FW-1366

Message `<timestamp>, [FW-1366], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of time service (TS) out-of-sync violations has risen above the high boundary.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1367

Message `<timestamp>, [FW-1367], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of time service (TS) out-of-sync violations has changed from a value outside of the acceptable range to a value within the acceptable range.

Recommended Action No action is required.

Severity INFO

FW-1368

Message `<timestamp>, [FW-1368], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of no-FCS violations has changed. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the world wide name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1369

Message `<timestamp>, [FW-1369], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of no-FCS violations has fallen below the low boundary. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the world wide name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action No action is required.

Severity INFO

FW-1370

Message `<timestamp>, [FW-1370], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of no-FCS violations has risen above the high boundary. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the world wide name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1371

Message `<timestamp>, [FW-1371], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of no-FCS violations has changed from a value outside of the acceptable range to a value within the acceptable range. This counter records how often the switch loses contact with the primary fabric configuration server (FCS) switch. When the primary FCS switch in the fabric sends its certificate to a switch, the receiving switch saves the world wide name (WWN) of that primary FCS switch. If a secure switch finds that there are no FCSs in the fabric, but it still has the WWN of the last primary FCS switch, it increments this counter and resets the WWN of the primary FCS to all zeroes.

Recommended Action No action is required.

Severity INFO

FW-1372

Message `<timestamp>, [FW-1372], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of incompatible security database violations has changed. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1373

Message `<timestamp>, [FW-1373], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of incompatible security database violations has fallen below the low boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended Action No action is required.

Severity INFO

FW-1374

Message `<timestamp>, [FW-1374], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of incompatible security database violations has risen above the high boundary. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1375

Message `<timestamp>, [FW-1375], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of incompatible security database violations has changed from a value outside of the acceptable range to a value within the acceptable range. This violation indicates the number of secure switches with different version stamps have been detected. When a switch is in secure mode, it connects only to another switch that is in secure mode and has a compatible security database. A compatible security database means that the version stamp and fabric configuration server (FCS) policy matches exactly.

Recommended Action No action is required.

Severity INFO

FW-1376

Message `<timestamp>, [FW-1376], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of illegal commands has changed. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity INFO

FW-1377

Message `<timestamp>, [FW-1377], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of illegal commands has fallen below the low boundary. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action No action is required.

Severity INFO

FW-1378

Message `<timestamp>, [FW-1378], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of illegal commands has risen above the high boundary. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action Responses to security-class messages depend on user policies. Consult your security administrator for response strategies and policies.

Severity WARNING

FW-1379

Message `<timestamp>, [FW-1379], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of illegal commands has changed from a value outside of the acceptable range to a value within the acceptable range. This counter tracks how many times commands allowed only on the primary fabric configuration server (FCS) switch have been executed on a non-primary FCS switch. There are many commands that can be executed only on the primary FCS switch as well as one security command that can be executed only on a backup FCS switch. The counter increments every time someone issues one of these commands on a switch where it is not allowed.

Recommended Action No action is required.

Severity INFO

FW-1400

Message `<timestamp>, [FW-1400], <sequence-number>,, INFO, <system-name>, <Label>, value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the flash usage percentage has changed. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1401

Message `<timestamp>, [FW-1401], <sequence-number>,, INFO, <system-name>, <Label>, is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the flash usage percentage has fallen below the low boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1402

Message `<timestamp>, [FW-1402], <sequence-number>,, WARNING, <system-name>, <Label>, is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the flash usage percentage has risen above the high boundary. Flash increases and decreases slightly with normal operation of the switch. Excessive permanent increases can lead to future problems.

Recommended Action You might have to remove some unwanted files to create some flash space. Run the **supportSave** command to remove files from the kernel space.

Severity WARNING

FW-1403

Message `<timestamp>, [FW-1403], <sequence-number>,, INFO, <system-name>, <Label>, is between high and low boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause It means some process is using more memory or cpu.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1404

Message `<timestamp>, [FW-1404], <sequence-number>,, WARNING, <system-name>, <Label>,is above high boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause It means CPU or memory usage is above its threshold. If this RASLOG is pertaining to memory usage then the usage is above middle memory threshold.

Recommended Action No action is required.

Severity WARNING

FW-1405

Message `<timestamp>, [FW-1405], <sequence-number>,, INFO, <system-name>, <Label>,is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause It means memory usage below low threshold.

Recommended Action No action is required.

Severity INFO

FW-1406

Message `<timestamp>, [FW-1406], <sequence-number>,, CRITICAL, <system-name>, <Label>,is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause It means memory usage is above high memory threshold.

Recommended Action No action is required.

Severity CRITICAL

FW-1407

Message `<timestamp>, [FW-1407], <sequence-number>,, INFO, <system-name>, <Label>,is between high boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause It means memory usage is between high and middle thresholds.

Recommended Action No action is required.

Severity INFO

FW-1408

Message `<timestamp>, [FW-1408], <sequence-number>,, INFO, <system-name>, <Label>,is between high boundaries(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause It means memory usage is between low and high or middle thresholds.

Recommended Action No action is required.

Severity INFO

FW-1424

Message `<timestamp>, [FW-1424], <sequence-number>,, WARNING, <system-name>, Switch status changed from <Previous state> to <Current state>.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because of a policy violation.

Recommended Action Run the **switchStatusShow** command to determine the policy violation.

Severity WARNING

FW-1425

Message `<timestamp>, [FW-1425], <sequence-number>,, INFO, <system-name>, Switch status changed from <Bad state> to HEALTHY.`

Probable Cause Indicates that the switch status has changed to a healthy state. This occurred because a policy is no longer violated.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1426

Message `<timestamp>, [FW-1426], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Power supply: <Number Bad> bad, <Number Missing> absent.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty or missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty or missing power supply.

Severity WARNING

FW-1427

Message `<timestamp>, [FW-1427], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Power supply: <Number Bad> bad.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty power supply.

Severity WARNING

FW-1428

Message `<timestamp>, [FW-1428], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Power supply: <Number Missing> absent.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of missing power supplies is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the missing power supply.

Severity WARNING

FW-1429

Message `<timestamp>, [FW-1429], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor: Power supplies are not redundant.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the power supplies are not in the correct slots for redundancy.

Recommended Action Rearrange the power supplies so that one is in an odd slot and other in an even slot to make them redundant.

Severity WARNING

FW-1430

Message `<timestamp>, [FW-1430], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor <string>.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty temperature sensors is greater than or equal to the policy set by the **switchStatusPolicySet** command. A temperature sensor is faulty when the sensor value is not in the acceptable range or is faulty.

Recommended Action Replace the field-replaceable unit (FRU) with the faulty temperature sensor.

Severity WARNING

FW-1431

Message `<timestamp>, [FW-1431], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Fan: <Number Bad> bad.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty fans is greater than or equal to the policy set by the **switchStatusPolicySet** command. A fan is faulty when sensor value is not in the acceptable range or is faulty.

Recommended Action Replace the faulty or deteriorating fan field-replaceable units (FRUs).

Severity WARNING

FW-1432

Message `<timestamp>, [FW-1432], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor WWN: <Number Bad> bad.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty world wide name (WWN) cards is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty WWN card.

Severity WARNING

FW-1433

Message `<timestamp>, [FW-1433], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor CP: CP non-redundant.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty CPs is greater than or equal to the policy set by the **switchStatusPolicySet** command. The CPs are non-redundant.

If you power cycle a Brocade 24000 chassis in dual-domain configuration, and then reset the micro-switch of the active CP before the heartbeat is up, this will cause both CPs to come up in a non-redundant state.

Recommended Action Run the **firmwareShow** command to verify that both CPs have compatible firmware levels. Run the **firmwareDownload** command to install the same level of firmware to both CPs. Replace any faulty CPs.

If you reset the micro-switch (the latch on the CP blade) on the active CP before the heartbeat was up on a power cycle, and the CPs came up non-redundant, then you should reboot the CPs again to clear the problem.

Severity WARNING

FW-1434

Message `<timestamp>, [FW-1434], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Blade: <Number Bad> blade failures.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of blade failures is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty blade.

Severity WARNING

FW-1435

Message `<timestamp>, [FW-1435], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Flash: usage out of range.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the flash usage is out of range. The policy was set using the **switchStatusPolicySet** command.

Recommended Action Run the **supportSave** command to clear out the kernel flash. Refer to the *Fabric OS Command Reference* for more information about this command.

Severity WARNING

FW-1436

Message `<timestamp>, [FW-1436], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Marginal ports: <Num of marginal ports and the port numbers> marginal ports. (Ports <Unknown>)`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of marginal ports is greater than or equal to the policy set using the **switchStatusPolicySet** command. A port is faulty when the port value for Link Loss, Synchronization Loss, Signal Loss, Invalid word, Protocol error, cyclic redundancy check (CRC) error, Port state change or Buffer Limited Port is above the high boundary.

Recommended Action Replace any faulty or deteriorating small form-factor pluggables (SFPs).

Severity WARNING

FW-1437

Message `<timestamp>, [FW-1437], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor faulty ports: <Num of faulty ports>. (Ports <unknown>.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of faulty ports is greater than or equal to the policy set by the **switchStatusPolicySet** command. A port is considered faulty due to hardware failure such as a faulty small form-factor pluggable (SFP) or port.

Recommended Action Replace any faulty or deteriorating small form-factor pluggables (SFPs).

Severity WARNING

FW-1438

Message `<timestamp>, [FW-1438], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Missing SFPs: <Num of missing SFPs> missing SFPs.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the number of missing small form-factor pluggables (SFPs) is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Run the **switchStatusPolicySet** command to modify the SFP policy or to add SFPs to the empty ports.

Severity WARNING

FW-1439

Message `<timestamp>, [FW-1439], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Switch offline.`

Probable Cause Indicates that the switch status is not in a healthy state. This occurred because the switch is offline.

Recommended Action Run the **switchEnable** command.

Severity WARNING

FW-1440

Message `<timestamp>, [FW-1440], <sequence-number>,, INFO, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to “absent”.

Recommended Action No action is required. Verify that the event was planned.

Severity INFO

FW-1441

Message `<timestamp>, [FW-1441], <sequence-number>,, INFO, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to “inserted”. This means that an FRU is inserted but not powered on.

Recommended Action No action is required. Verify that the event was planned.

Severity INFO

FW-1442

Message `<timestamp>, [FW-1442], <sequence-number>,, INFO, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to “on”.

Recommended Action No action is required. Verify that the event was planned.

Severity INFO

FW-1443

Message `<timestamp>, [FW-1443], <sequence-number>,, INFO, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) changed to “off”.

Recommended Action No action is required. Verify that the event was planned.

Severity INFO

FW-1444

Message `<timestamp>, [FW-1444], <sequence-number>,, WARNING, <system-name>, <FRU label> state has changed to <FRU state>.`

Probable Cause Indicates that the state of the specified field-replaceable unit (FRU) has changed to “faulty”.

Recommended Action Replace the FRU.

Severity WARNING

FW-1445

Message `<timestamp>, [FW-1445], <sequence-number>,, INFO, <system-name>, Four power supplies are now required for 2X redundancy, Switch Status Policy values changed.`

Probable Cause Indicates that the switch now requires 4 power supplies and previous Switch Status Policy parameters will be overwritten to reflect this. The presence of an AP blade means that more than one power supply may be required to provide adequate power. So (even if the AP blade is powered down or removed) the Switch Status policy values will now reflect the need for 4 power supplies to maintain full (2X) redundancy.

Recommended Action No action required, unless there are fewer than 4 power supplies active in the chassis. If there are fewer than 4, insert additional power supplies so that there are 4 active.

Severity INFO

FW-1446

Message `<timestamp>, [FW-1446], <sequence-number>,, WARNING, <system-name>, Four power supplies now required for 2X redundancy, not enforced by Fabric Watch due to Switch Status Policy overridden by User.`

Probable Cause Indicates that the switch now requires 4 power supplies for full (2X) redundancy, but the user has previously overridden the Switch Status Policy values pertaining to number of power supplies. So those values will not be automatically changed. The default values with no AP blades are: 3 out of service indicates switch status is DOWN, 0 indicates no checking for switch status MARGINAL. The default values when an AP blade is or has been present are: 2 out of service indicates switch status is DOWN, 1 out of service indicates switch status is MARGINAL

Recommended Action To maintain full (2X) redundancy and proper monitoring by Fabric Watch, 4 active power supplies should be supplied and the default values associated with the presence of an AP blade should be entered with **switchStatusPolicyset** command.

Severity WARNING

FW-1447

Message `<timestamp>, [FW-1447], <sequence-number>,, WARNING, <system-name>, Switch status change contributing factor Core Blade: <Number Bad> Core blade failures (<Switch State>).`

Probable Cause Indicates that the switch is not in a healthy state. This occurred because the number of core blade failures is greater than or equal to the policy set by the **switchStatusPolicySet** command.

Recommended Action Replace the faulty core blade.

Severity WARNING

FW-1500

Message `<timestamp>, [FW-1500], <sequence-number>,, WARNING, <system-name>, Mail overflow - Alerts being discarded.`

Probable Cause Indicates that mail alert overflow condition has occurred.

Recommended Action Resolve or disable the mail alert using the **fwMailCfg** command.

Severity WARNING

FW-1501

Message `<timestamp>, [FW-1501], <sequence-number>,, INFO, <system-name>, Mail overflow cleared - <Mails discarded> alerts discarded.`

Probable Cause Indicates that the mail overflow condition has cleared.

Recommended Action No action is required.

Severity INFO

FW-1510

Message `<timestamp>, [FW-1510], <sequence-number>,, INFO, <system-name>, <Area string> threshold exceeded: Port <Port number> disabled.`

Probable Cause It means port has been fenced because port has violated CRC, ITW, PE, C3TX_TO, ST, and LR high thresholds.

Recommended Action Check for concurrent loss of synchronization errors. Check the SFP and the cable. Then enable the port using the **portEnable** command.

Severity INFO

FW-1511

Message `<timestamp>, [FW-1511], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of link failures that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1512

Message `<timestamp>, [FW-1512], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of link failures that the port experiences has changed and dropped below upper threshold boundary to a value within the acceptable range. Link loss errors occur when a link experiences a loss of signal and fails. Both physical and hardware problems can cause link loss errors. Link loss errors frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot them.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1513

Message

```
<timestamp>, [FW-1513], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary threshold boundary to in
between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of synchronization losses that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1514

Message

```
<timestamp>, [FW-1514], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has dropped below upper threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of synchronization losses that the port experiences has changed and dropped below upper threshold boundary to a value within the acceptable range. Loss of synchronization errors frequently occur due to a faulty small form-factor pluggable (SFP) or cable. Signal losses often create synchronization losses.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1515

Message

```
<timestamp>, [FW-1515], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary to in between(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of signal losses that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range. Loss of signal generally indicates a physical problem.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent loss of signal generally indicates a physical problem. Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Severity INFO

FW-1516

Message

```
<timestamp>, [FW-1516], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has dropped below upper threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of signal losses that the port experiences has changed and dropped below upper threshold boundary to a value within the acceptable range. Loss of signal generally indicates a physical problem.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent loss of signal generally indicates a physical problem. Check both ends of your cable connection. Verify that the cable and small form-factor pluggables (SFPs) are not faulty.

Severity INFO

FW-1517

Message

```
<timestamp>, [FW-1517], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary to in between(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of protocol errors that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1518

Message

```
<timestamp>, [FW-1518], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has dropped below upper threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of protocol errors that the port experiences has changed and dropped below upper threshold boundary to a value within the acceptable range. Occasional protocol errors occur due to software glitches. Persistent protocol errors occur due to hardware problems.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1519

Message

```
<timestamp>, [FW-1519], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary to in between(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of invalid words that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range. Invalid words usually indicate a hardware problem with a small form-factor pluggable (SFP) or cable.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1520

Message

```
<timestamp>, [FW-1520], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has dropped below upper threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of invalid words that the port experiences has changed and dropped below upper threshold boundary to a value within the acceptable range. Invalid words usually indicate a hardware problem with a small form-factor pluggable (SFP) or cable.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1521

Message

```
<timestamp>, [FW-1521], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary to in between(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences crossed lower threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity INFO

FW-1522

Message

```
<timestamp>, [FW-1522], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary to in between(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of invalid cyclic redundancy checks (CRCs) that the port experiences has dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation. Frequent fluctuations in CRC errors generally indicate an aging fabric. Check your small form-factor pluggables (SFPs), cables, and connections for faulty hardware. Verify that all optical hardware is clean.

Severity INFO

FW-1523

Message

```
<timestamp>, [FW-1523], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary to in between(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1524

Message

```
<timestamp>, [FW-1524], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has dropped below upper threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the percentage of incoming traffic that the port experiences has changed and dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1525

Message `<timestamp>, [FW-1525], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1526

Message `<timestamp>, [FW-1526], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the percentage of outgoing traffic that the port experiences has changed and dropped below upper threshold boundary to a value within the acceptable range.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1527

Message `<timestamp>, [FW-1527], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of state changes that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1528

Message `<timestamp>, [FW-1528], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of state changes that the port experiences has changed and dropped below upper boundary to a value within the acceptable range. The state of the port has changed for one of the following reasons: the port has gone offline, has come online, is testing, is faulty, has become an E_Port, has become an F_Port, has segmented, or has become a trunk port.

Recommended Action No action is required. Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1529

Message

```
<timestamp>, [FW-1529], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary to in between(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of link resets that the port experiences has changed and crossed lower threshold boundary to a value within the acceptable range. Link resets occur due to link timeout errors that indicate no frame activity at all. Both physical and hardware problems can cause link resets to increase.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1530

Message

```
<timestamp>, [FW-1530], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has dropped below upper threshold boundary to in between(High=<High
value>, Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of link resets that the port experiences has changed and dropped below upper threshold boundary to a value within the acceptable range. Link resets occur due to link timeout errors that indicate no frame activity at all. Both physical and hardware problems can cause link resets to increase.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-1531

Message

```
<timestamp>, [FW-1531], <sequence-number>,, INFO, <system-name>, <Port Name>,
<Label>, has crossed lower threshold boundary to in between(High=<High value>,
Low=<Low value>). Current value is <Value> <Unit>.
```

Probable Cause Indicates that the number of C3 transmit time out frames has crossed lower threshold boundary and is in between low and high thresholds.

Recommended Action Check the target device. It could be slow.

Severity INFO

FW-1532

Message `<timestamp>, [FW-1532], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has dropped below upper threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the number of C3 transmit time out frames has dropped below upper threshold boundary and is in between low and high thresholds.

Recommended Action Check the target device. It could be slow.

Severity INFO

FW-1533

Message `<timestamp>, [FW-1533], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has crossed lower threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the trunk utilization crossed lower threshold boundary to in between low and high thresholds.

Recommended Action No action is required.

Severity INFO

FW-1534

Message `<timestamp>, [FW-1534], <sequence-number>,, INFO, <system-name>, <Port Name>, <Label>, has dropped below threshold boundary to in between(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the trunk utilization has dropped below upper threshold boundary to in between low and high thresholds.

Recommended Action No action is required.

Severity INFO

FW-1535

Message `<timestamp>, [FW-1535], <sequence-number>,, INFO, <system-name>, Fabric Watch has stopped portfencing feature for <Area String> loss area in <Port Name> class since FOS6.3. Disabling port fencing feature for this.`

Probable Cause Indicates that in previous versions portfencing is configured for Link/Sync loss, but after upgrading to new version, in which portfencing is not suppoted, resets the above bit.

Recommended Action No action is required. You are informed that PF bit is reset.

Severity INFO

FW-3010

Message `<timestamp>, [FW-3010], <sequence-number>,, INFO, <system-name>, <Port Name>,<Label> value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the circuit utilization has changed.

Recommended Action Respond to this message as it is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-3011

Message `<timestamp>, [FW-3011], <sequence-number>,, INFO, <system-name>, <Port Name>,<Label> is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the circuit utilization is below threshold.

Recommended Action No action is required.

Severity INFO

FW-3012

Message `<timestamp>, [FW-3012], <sequence-number>,, WARNING, <system-name>, <Port Name>,<Label> is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates that the circuit utilization is above threshold.

Recommended Action No action is required.

Severity WARNING

FW-3013

Message `<timestamp>, [FW-3013], <sequence-number>,, INFO, <system-name>, <Port Name>,<Label> is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>`

Probable Cause Indicates that the circuit utilization is in-between high and low threshold.

Recommended Action No action required.

Severity INFO

FW-3014

Message `<timestamp>, [FW-3014], <sequence-number>,, INFO, <system-name>, <Port Name>,<Label> value has changed(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>.`

Probable Cause Indicates the packet loss that the circuit experiences has changed.

Recommended Action Respond to this message as it is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-3015

Message `<timestamp>, [FW-3015], <sequence-number>,, INFO, <system-name>, <Port Name>,<Label> is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>`

Probable Cause Indicates the packet loss that the circuit experiences is below threshold.

Recommended Action No action is required.

Severity INFO

FW-3016

Message `<timestamp>, [FW-3016], <sequence-number>,, WARNING, <system-name>, <Port Name>,<Label> is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>`

Probable Cause Indicates the packet loss that the circuit experiences is above threshold.

Recommended Action No action is required.

Severity WARNING

FW-3017

Message

```
<timestamp>, [FW-3017], <sequence-number>,, INFO, <system-name>, <Port
Name>,<Label> is between high and low boundary(High=<High value>, Low=<Low
value>). Current value is <Value> <Unit>
```

Probable Cause Indicates the packet loss that the circuit experiences is in-between the specified range.

Recommended Action No action is required.

Severity INFO

FW-3018

Message

```
<timestamp>, [FW-3018], <sequence-number>,, INFO, <system-name>, <Port
Name>,<Label> value has changed(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>
```

Probable Cause Indicates the number of state changes that the circuit experiences has changed. The state of the circuit has changed for either of the reason that if the circuit has gone offline or it has come online.

Recommended Action Respond to this message as is appropriate to the particular policy of the end-user installation.

Severity INFO

FW-3019

Message

```
<timestamp>, [FW-3019], <sequence-number>,, INFO, <system-name>, <Port
Name>,<Label> is below low boundary(High=<High value>, Low=<Low value>). Current
value is <Value> <Unit>
```

Probable Cause Indicates the number of state changes that the circuit experiences has reduced below the low boundary level. The state of the circuit has changed for either of the reason that if the circuit has gone offline or it has come online.

Recommended Action No action is required.

Severity INFO

FW-3020

Message `<timestamp>, [FW-3020], <sequence-number>,, WARNING, <system-name>, <Port Name>,<Label> is above high boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>`

Probable Cause Indicates the number of state changes that the circuit experiences has increased above the high boundary. The state of the circuit has changed for the reason that the circuit has gone offline, it has come online, or it is testing.

Recommended Action No action is required.

Severity WARNING

FW-3021

Message `<timestamp>, [FW-3021], <sequence-number>,, WARNING, <system-name>, <Port Name>,<Label> is below low boundary(High=<High value>, Low=<Low value>). Current value is <Value> <Unit>`

Probable Cause Indicates the number of state changes that the circuit experiences has increased above the high boundary. The state of the circuit has changed for the reason that the circuit has gone offline, it has come online, or is testing.

Recommended Action No action is required.

Severity WARNING

Chapter

HAM System Messages

43

HAM-1001

Message `<timestamp>, [HAM-1001], <sequence-number>, SLOT cp-slpt-number | FFDC | CHASSIS, FFDC, CRITICAL, <system-name>, Standby CP is not healthy, device <device name> status BAD, Severity = <Log="YES" Class="NONE" Severity>`

Probable Cause Indicates that a standby control processor (CP) device error is reported by the high-availability manager (HAM) Health Monitor, with a specific device and Log="YES" Class="NONE" Severity level. The *severity level* can be "critical", "major", or "minor".

The active CP will continue to function normally, but because the standby CP is not healthy, non-disruptive failover is not possible.

Recommended Action Reboot the standby CP blade by ejecting the card and reseating it. If the problem persists, replace the standby CP. Run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

HAM-1002

Message `<timestamp>, [HAM-1002], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, Standby CP is healthy.`

Probable Cause Indicates that all of the standby control processor (CP) devices monitored by the high-availability manager (HAM) Health Monitor report no error.

Recommended Action No action is required.

Severity INFO

HAM-1004

Message `<timestamp>, [HAM-1004], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, Processor rebooted - <Reboot Reason>.`

Probable Cause Indicates the system has been rebooted either because of a user action or an error. The switch reboot can be initiated by the **firmwareDownload, fastBoot, haFailover,** and **reboot** commands. Some examples of errors that might initiate this message are hardware errors, software errors, compact flash errors, or memory errors. The *reboot reasons* can be any of the following:

- Hafailover
- Reset

- Fastboot
- Giveup Master:SYSM
- CP Faulty:SYSM
- FirmwareDownload
- ConfigDownload:MS
- ChangeWWN:EM
- Reboot:WebTool
- Fastboot:WebTool
- Software Fault:Software Watchdog
- Software Fault:Kernel Panic
- Software Fault:ASSERT
- Reboot:SNMP
- Fastboot:SNMP
- Reboot
- Chassis Config
- Reboot:API
- Reboot:HAM
- EMFault:EM

Recommended Action Check the error log on both CPs for additional messages that might indicate the reason for the reboot.

Severity INFO

HAM-1005

Message `<timestamp>, [HAM-1005], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, HeartBeat Miss reached threshold.`

Probable Cause Indicates that either the active control processor (CP) EMAC controller or the standby CP is down. The active CP will run a diagnostic test on the EMAC controller and will wait for the standby CP to reset it if it is down.

Recommended Action No action is required.

Severity INFO

HAM-1006

Message `<timestamp>, [HAM-1006], <sequence-number>, SLOT cp-slpt-number | FFDC | CHASSIS, FFDC, CRITICAL, <system-name>,EMAC controller for Active CP is BAD.`

Probable Cause Indicates that the local EMAC controller on the active control processor (CP) is BAD as determined by the diagnostic test run by the HAM module.

Recommended Action The standby CP will take over and reset the active CP. The system will be non-redundant as the standby becomes the active CP. Run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

HAM-1007

Message `<timestamp>, [HAM-1007], <sequence-number>, SLOT cp-slpt-number | FFDC | CHASSIS, FFDC, CRITICAL, <system-name>,Need to reboot the system for recovery, reason: <reason name>.`

Probable Cause Indicates that the system in current condition needs to be rebooted to achieve a reliable recovery. The reasons can be that the standby CP is not ready when failover occurred, failover happened when the last LS transaction is incomplete, or the system failed when a timeout occurred at certain stage or cold/warm recovery failed. If auto-reboot is enabled, the system will automatically reboot itself. Otherwise you need to manually reboot it.

Recommended Action For a reliable recovery, reboot the system manually if auto-reboot recovery is disabled. Run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

HAM-1008

Message `<timestamp>, [HAM-1008], <sequence-number>, SLOT cp-slpt-number | FFDC | CHASSIS, FFDC, CRITICAL, <system-name>,Rebooting the system for recovery - auto-reboot is enabled.`

Probable Cause Indicates that recovery by reboot is enabled, the system will automatically reboot itself. This follows if the event logged in 1007 has happened and auto-reboot is enabled.

Recommended Action No action is required.

Severity CRITICAL

HAM-1009

Message `<timestamp>, [HAM-1009], <sequence-number>, SLOT cp-slpt-number | FFDC | CHASSIS, FFDC, CRITICAL, <system-name>,Need to MANUALLY REBOOT the system for recovery - auto-reboot is disabled.`

Probable Cause Indicates that recovery by reboot is disabled, the system needs to be manually rebooted for recovery. This follows if the event logged in 1007 has happened and auto-reboot is disabled.

Recommended Action Reboot the whole system manually to recover.

Severity CRITICAL

HAM-1010

Message `<timestamp>, [HAM-1010], <sequence-number>, SLOT cp-slot-number | CHASSIS, CRITICAL, <system-name>,Please maunually trigger hareboot/reboot for recovery from OOM when appropriate.`

Probable Cause Indicates OOM is detected when system is not ready for warm recovery.

Recommended Action Manually trigger reboot for cold recovery if needed, or wait until system is ready and use hareboot/hafailover to trigger warm recovery.

Severity CRITICAL

HAM-1011

Message `<timestamp>, [HAM-1011], <sequence-number>, SLOT cp-slot-number | CHASSIS, CRITICAL, <system-name>,Hareboot is automatically triggered for warm recovery from OOM.`

Probable Cause Indicates OOM is detected when system is ready for warm recovery. Hareboot is automatically triggered.

Recommended Action No action is required.

Severity CRITICAL

HAM-1012

Message `<timestamp>, [HAM-1012], <sequence-number>, SLOT cp-slot-number | CHASSIS, CRITICAL, <system-name>,Password database conversion failed.`

Probable Cause Indicates the password database conversion failed.

Recommended Action No action is required.

Severity CRITICAL

HAM-1013

Message `<timestamp>, [HAM-1013], <sequence-number>, SLOT cp-slot-number | CHASSIS, CRITICAL, <system-name>.`

Probable Cause Indicates a software watchdog detected termination of a restartable daemon, but could not restart it.

Recommended Action If needed manually initiate a reboot/failover.

Severity CRITICAL

HAM-1014

Message `<timestamp>, [HAM-1014], <sequence-number>, SLOT cp-slot-number | CHASSIS, CRITICAL, <system-name>.`

Probable Cause Indicates a software watchdog detected termination of a restartable daemon and needed to reboot/failover.

Recommended Action If needed manually initiate a reboot/failover.

Severity CRITICAL

43 HAM-1014

Chapter

HAMK System Messages

44

HAMK-1001

Message `<timestamp>, [HAMK-1001], <sequence-number>, SLOT cp-slot-number | CHASSIS, FFDC, CRITICAL, <system-name>, Warm recovery failed.`

Probable Cause Indicates the switch failed during the warm recovery.

Recommended Action This message triggers a switch reboot automatically and attempts a cold recovery. Run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

HAMK-1002

Message `<timestamp>, [HAMK-1002], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, Heartbeat down.`

Probable Cause Indicates that the active control processor (CP) blade determined that the standby CP blade is down. This can be a result of an operator-initiated action such as the **firmwareDownload** command, the standby CP blade being reset or removed, of an error in the standby CP blade.

Recommended Action Monitor the standby CP blade for a few minutes. If this message is due to a standby CP reboot, the message HAMK-1003 will display after the standby CP has completed the reboot successfully.

If the standby CP does not successfully connect to the active CP after 10 minutes, reboot the standby CP blade by ejecting the blade and reseating it.

Severity INFO

HAMK-1003

Message `<timestamp>, [HAMK-1003], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, Heartbeat up.`

Probable Cause Indicates that the active control processor (CP) blade detects the standby CP blade. This message indicates that the standby CP blade is available to take over in case a failure happens on the active CP blade.

Recommended Action No action is required. This message means that the standby CP is healthy.

Severity INFO

HAMK-1004

Message `<timestamp>,[HAMK-1004], <sequence-number>, SLOT cp-slot-number | CHASSIS, INFO, <system-name>, Resetting standby CP (double reset may occur).`

Probable Cause Indicates that the standby control processor (CP) is being reset due to a loss of heartbeat. This message is typically seen when the standby CP has been rebooted. Note that in certain circumstances a CP may experience a double reset and reboot twice in a row. A CP can recover automatically even if it has rebooted twice.

Recommended Action No action is required.

Severity INFO

Chapter

HIL System Messages

45

HIL-1101

Message `<timestamp>, [HIL-1101], <sequence-number>,, ERROR, <system-name>, Slot <slot number> faulted, <nominal voltage> (<measured voltage>) is above threshold.`

Probable Cause Indicates that the blade voltage is above threshold.

Recommended Action Replace the faulty blade or switch (for nonbladed switches).

Severity ERROR

HIL-1102

Message `<timestamp>, [HIL-1102], <sequence-number>,, ERROR, <system-name>, Slot <slot number> faulted, <nominal voltage> (<measured voltage>) is below threshold.`

Probable Cause Indicates that the blade voltage is below threshold.

Recommended Action Replace the faulty blade or switch (for nonbladed switches).

Severity ERROR

HIL-1103

Message `<timestamp>, [HIL-1103], <sequence-number>,, ERROR, <system-name>, Blower <blower number> faulted, <nominal voltage> (<measured voltage>) is above threshold.`

Probable Cause Indicates that the fan voltage is above threshold.

Recommended Action Run the **psShow** command to verify the power supply status.

Try to reseat the faulty fan field-replaceable units (FRUs) and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

Severity ERROR

HIL-1104

Message `<timestamp>, [HIL-1104], <sequence-number>,, ERROR, <system-name>, Blower <blower number> faulted, <nominal voltage> (<measured voltage>) is below threshold.`

Probable Cause Indicates that the fan voltage is below threshold.

Recommended Action Run the **psShow** command to verify the power supply status.

Try to reseat the faulty fan field-replaceable units (FRUs) and power supply FRU to verify that they are seated properly.

If the problem persists, replace the fan FRU or the power supply FRU as necessary.

Severity ERROR

HIL-1105

Message `<timestamp>, [HIL-1105], <sequence-number>,, ERROR, <system-name>, Switch error, <nominal voltage> (<measured voltage>) above threshold.`

Probable Cause Indicates that the switch voltage is above threshold. This message is specific to nonbladed switches and is not applicable to the Brocade 24000 or 48000.

Recommended Action For the Brocade 200E, 3250, 3850, 4012, 4016, 4018, 4020, and 4024, the entire switch must be replaced because these switches do not have field-replaceable units (FRUs).

For the Brocade 3900, replace the motherboard FRU.

For the Brocade 4100 , 4900, 7500, and AP7600, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

Severity ERROR

HIL-1106

Message `<timestamp>, [HIL-1106], <sequence-number>,, ERROR, <system-name>, Switch error, <nominal voltage> (<measured voltage>) below threshold.`

Probable Cause Indicates that the switch voltage is below threshold. This message is specific to nonbladed switches and is not applicable to the Brocade 24000 or 48000.

Recommended Action For the Brocade 200E, 3250, 3850, 4012, 4016, 4018, 4020, and 4024, the entire switch must be replaced because these switches do not have field-replaceable units (FRUs).

For the Brocade 3900, replace the motherboard FRU.

For the Brocade 4100, 4900, 7500, and AP7600, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

Severity ERROR

HIL-1107

Message `<timestamp>, [HIL-1107], <sequence-number>, FFDC, ERROR, <system-name>, Switch faulted, <nominal voltage> (<measured voltage>)above threshold.`

Probable Cause Indicates that the switch voltage is above threshold. This message is specific to nonbladed switches and is not applicable to the Brocade 24000 or 48000.

Recommended Action For the Brocade 200E, 3250, 3850, 4012, 4016, 4018, 4020, and 4024, the entire switch must be replaced because these switches do not have field-replaceable units (FRUs).

For the Brocade 3900, replace the motherboard FRU.

For the Brocade 4100, 4900, 7500, and AP7600, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

Severity ERROR

HIL-1108

Message `<timestamp>, [HIL-1108], <sequence-number>, FFDC, CRITICAL, <system-name>, Switch faulted, <nominal voltage> (<measured voltage>) below threshold. System preparing for reset.`

Probable Cause Indicates that the switch voltage is below threshold. This message is specific to nonbladed switches and is not applicable to the Brocade 24000 or 48000.

Recommended Action For the Brocade 200E, 3250, 3850, 4012, 4016, 4018, 4020, and 4024, the entire switch must be replaced because these switches do not have field-replaceable units (FRUs).

For the Brocade 3900, replace the motherboard FRU.

For the Brocade 4100, 4900, 7500, and AP7600, if the 12 volt level is faulty, replace one or both power supplies; if any other voltage is faulty, replace the entire switch.

Severity CRITICAL

HIL-1201

Message `<timestamp>, [HIL-1201], <sequence-number>,, WARNING< <system-name>, Blower <blower number>, speed (<measured speed> RPM) above threshold.`

Probable Cause Indicates that the fan speed (in RPMs) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action Run the **tempShow** command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan FRU.

Severity WARNING

HIL-1202

Message `<timestamp>, [HIL-1202], <sequence-number>,, ERROR, <system-name>, Blower <blower number> faulted, speed (<measured speed> RPM) below threshold.`

Probable Cause Indicates that the specified fan speed (in RPMs) has fallen below the minimum threshold.

Recommended Action Replace the fan field-replaceable unit (FRU).

Severity ERROR

HIL-1203

Message `<timestamp>, [HIL-1203], <sequence-number>,, ERROR, <system-name>, Fan <fan number> faulted, speed (<measured speed> RPM) above threshold.`

Probable Cause Indicates that the specified fan speed (in RPMs) has risen above the maximum threshold. A high speed does not necessarily mean that the fan is faulty.

Recommended Action Run the **tempShow** command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Run the **fanShow** command to monitor the speed of the fan generating this error.

If the fan continues to generate this message, replace the fan FRU.

Severity ERROR

HIL-1204

Message `<timestamp>, [HIL-1204], <sequence-number>,, ERROR, <system-name>, Fan <fan number> faulted, speed (<measured speed> RPM) below threshold.`

Probable Cause Indicates that the specified fan speed (in RPMs) has fallen below the minimum threshold. This message is specific to nonbladed switches and is not applicable to the Brocade 24000 or 48000.

Recommended Action For the Brocade 3900 replace the fan FRU.

For the Brocade 3016, 3250 and 3850, the entire switch must be replaced because these switches do not have field-replaceable units (FRUs).

Severity ERROR

HIL-1206

Message `<timestamp>, [HIL-1206], <sequence-number>,, ERROR, <system-name>, Fan <fan number> sensor <sensor number> , speed (<measured speed> RPM) below threshold.`

Probable Cause Indicates that the specified fan speed (in RPMs) has fallen below the minimum threshold. This problem can quickly cause the switch to overheat. This message is specific to nonbladed switches and is not applicable to the Brocade 24000 or 48000.

Recommended Action For the Brocade 4100, 4900, 7500, and AP7600, replace the fan field-replaceable unit (FRU).

Severity ERROR

HIL-1207

Message `<timestamp>, [HIL-1207], <sequence-number>,, ERROR, <system-name>, Fan <fan number> is faulty.`

Probable Cause Indicates that the fan is faulty.

Recommended Action Use the **tempShow** command to verify that the switch temperatures are within operational ranges. Refer to the hardware reference manual for the temperature range of your switch.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Use the **fanShow** command to monitor the status of the fan generating this error.

If the fan continues to generate this message, replace the switch because the fan is not field-replaceable.

Severity ERROR

HIL-1208

Message `<timestamp>, [HIL-1208], <sequence-number>,, INFO, <system-name>, Fan <fan number> is not faulty.`

Probable Cause Indicates that the fan is not faulty.

Recommended Action This can only occur on switches with non-removable fans. It follows a previous indication of faultiness.

If the fan continues to generate this message, it indicates oscillation between faulty and non-faulty behavior. Replace the switch because the fan is not field-replaceable.

Severity INFO

HIL-1301

Message `<timestamp>, [HIL-1301], <sequence-number>,, WARNING, <system-name>, 1 blower failed or missing. Replace failed or missing blower assembly immediately.`

Probable Cause Indicates that a fan field-replaceable unit (FRU) has failed or has been removed. This message is often preceded by a low speed error message. This problem can cause the switch to overheat.

Recommended Action Replace the affected fan FRU immediately.

Severity WARNING

HIL-1302

Message `<timestamp>, [HIL-1302], <sequence-number>,, WARNING, <system-name>, <count> blowers failed or missing. Replace failed or missing blower assemblies immediately.`

Probable Cause Indicates that multiple fan field-replaceable unit (FRU)s have failed or are missing on a switch. This message is often preceded by a low fan speed message.

Recommended Action Replace the affected fan FRUs immediately.

Severity WARNING

HIL-1303

Message `<timestamp>, [HIL-1303], <sequence-number>,, ERROR, <system-name>, One fan failed. Replace failed fan FRU immediately.`

Probable Cause Indicates that a fan field-replaceable unit (FRU) has failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRU immediately

Severity ERROR

HIL-1304

Message `<timestamp>, [HIL-1304], <sequence-number>,, ERROR, <system-name>, Two fans failed. Replace failed fan FRUs immediately.`

Probable Cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRUs immediately.

Severity ERROR

HIL-1305

Message `<timestamp>, [HIL-1305], <sequence-number>,, ERROR, <system-name>, One or two fans failed. Replace failed fan FRUs immediately.`

Probable Cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRUs immediately.

Severity ERROR

HIL-1306

Message `<timestamp>, [HIL-1306], <sequence-number>,, ERROR, <system-name>, Three fans failed. Replace failed fan FRUs immediately.`

Probable Cause Indicates that three fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRUs immediately.

Severity ERROR

HIL-1307

Message `<timestamp>, [HIL-1307], <sequence-number>,, ERROR, <system-name>, Four or five fans failed. Replace failed fan FRUs immediately.`

Probable Cause Indicates that multiple fan field-replaceable units (FRUs) have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan FRUs immediately.

Severity ERROR

HIL-1308

Message `<timestamp>, [HIL-1308], <sequence-number>,, ERROR, <system-name>, All fans failed. Replace failed fan FRUs immediately.`

Probable Cause Indicates that all fans have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan field-replaceable units (FRUs) immediately.

Severity ERROR

HIL-1309

Message `<timestamp>, [HIL-1309], <sequence-number>,, ERROR, <system-name>, <count> fan FRUs failed. Replace failed fan FRUs immediately.`

Probable Cause Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended Action Replace the faulty fan field-replaceable unit (FRU)s immediately.

Severity ERROR

HIL-1310

Message `<timestamp>, [HIL-1310], <sequence-number>,, WARNING, <system-name>, <count> fans faulty.`

Probable Cause Indicates that multiple fans have failed. This message is often preceded by a low fan speed message.

Recommended Action Since the fans are not field replaceable, replace the switch if the temperature is high.

Severity WARNING

HIL-1311

Message `<timestamp>, [HIL-1311], <sequence-number>,, INFO, <system-name>, No fans are faulty.`

Probable Cause Indicates recovery from earlier condition of one or more fans having failed.

Recommended Action This can only occur on switches with non-removable fans. It follows a previous indication of faultiness.

If the fan continues to generate this message, it indicates oscillation between faulty and non-faulty behavior. Replace the switch because the fan is not field-replaceable.

Severity INFO

HIL-1401

Message `<timestamp>, [HIL-1401], <sequence-number>,, WARNING, <system-name>, One fan FRU missing. Install fan FRU immediately.`

Probable Cause Indicates that one fan field-replaceable unit (FRU) has been removed.

Recommended Action Install the missing fan FRU.

Severity WARNING

HIL-1402

Message `<timestamp>, [HIL-1402], <sequence-number>,, WARNING, <system-name>, Two fan FRUs missing. Install fan FRUs immediately.`

Probable Cause Indicates that two fan field-replaceable units (FRUs) have been removed.

Recommended Action Install the missing fan FRUs immediately.

Severity WARNING

HIL-1403

Message `<timestamp>, [HIL-1403], <sequence-number>,, WARNING, <system-name>, All fan FRUs missing. Install fan FRUs immediately.`

Probable Cause Indicates that all fan field-replaceable units (FRUs) have been removed.

Recommended Action Install the missing fan FRUs immediately.

Severity WARNING

HIL-1404

Message `<timestamp>, [HIL-1404], <sequence-number>,, WARNING, <system-name>, <count> fan FRUs missing. Install fan FRUs immediately.`

Probable Cause Indicates that one or more fan field-replaceable units (FRUs) have been removed.

Recommended Action Install the missing fan FRUs immediately.

Severity WARNING

HIL-1501

Message `<timestamp>, [HIL-1501], <sequence-number>,, WARNING, <system-name>, Slot <slot number>, high temperature (<measured temperature>).`

Probable Cause Indicates that the temperature of this blade has risen above the warning threshold.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity WARNING

HIL-1502

Message `<timestamp>, [HIL-1502], <sequence-number>, FFDC, CRITICAL, <system-name>, Slot <slot number>, high temperature (<measured temperature>). Unit will be shut down in 2 minutes if temperature remains high.`

Probable Cause Indicates that the temperature of this blade has risen above the critical threshold. This usually follows a high-temperature message.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the blade.

Severity CRITICAL

HIL-1503

Message `<timestamp>, [HIL-1503], <sequence-number>, FFDC, CRITICAL, <system-name>, Slot <slot number>, unit shutting down.`

Probable Cause Indicates that the temperature of this blade has been above the maximum threshold for at least two minutes. The blade is shut down to prevent damage. This usually follows a high-temperature warning message.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

If the message persists, replace the faulty blade.

Severity CRITICAL

HIL-1504

Message `<timestamp>, [HIL-1504], <sequence-number>,, INFO, <system-name>, System within normal temperature specifications (<measured temperature> C).`

Probable Cause Indicates that temperatures in the system have returned to normal.

Recommended Action No action is required.

Severity INFO

HIL-1505

Message `<timestamp>, [HIL-1505], <sequence-number>,, WARNING, <system-name>, High temperature (<measured temperature> C) fan speed increasing per environmental specifications.`

Probable Cause Indicates that temperatures in the system have risen above the warning threshold and the fan speed is increased.

Recommended Action Run the **fanShow** command to verify all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity WARNING

HIL-1506

Message `<timestamp>, [HIL-1506], <sequence-number>, FFDC, CRITICAL, <system-name>, High temperature (<measured temperature> C) exceeds system temperature limit. System will shut down within 2 minutes.`

Probable Cause Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action Run the **fanShow** command to verify that all fans are working properly. Replace any deteriorating fan field-replaceable units (FRUs).

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity CRITICAL

HIL-1507

Message `<timestamp>, [HIL-1507], <sequence-number>, FFDC, CRITICAL, <system-name>, High temperature warning time expired. System preparing for shutdown.`

Probable Cause Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity CRITICAL

HIL-1508

Message `<timestamp>, [HIL-1508], <sequence-number>, FFDC, CRITICAL, <system-name>, Fan faulty warning time expired. System preparing for shutdown.`

Probable Cause Indicates that temperatures in the system have remained above the critical threshold too long.

Recommended Action To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity CRITICAL

HIL-1509

Message `<timestamp>, [HIL-1509], <sequence-number>, FFDC, CRITICAL, <system-name>, High temperature (<measured temperature> C). Warning time expired. System preparing for shutdown.`

Probable Cause Indicates that temperatures in the system have risen above the critical threshold.

Recommended Action To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity CRITICAL

HIL-1510

Message `<timestamp>, [HIL-1510], <sequence-number>,, WARNING, <system-name>, Current temperature (<measured temperature> C) is below shutdown threshold. System shutdown cancelled.`

Probable Cause Indicates that temperatures in the system have dropped below the critical threshold; the system can continue operation.

Recommended Action To help prevent future problems, make sure that all the fans are working properly.

Make sure that the area is well-ventilated and that the room temperature is within operational range of your switch. Refer to the hardware reference manual for your switch for the operational temperature range.

Severity WARNING

HIL-1601

Message `<timestamp>, [HIL-1601], <sequence-number>,, ERROR, <system-name>, Using backup temperature sensor. Attention needed.`

Probable Cause Indicates that temperature readings from the primary sensor are out of range.

Recommended Action Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan field-replaceable units (FRUs).

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

Severity ERROR

HIL-1602

Message `<timestamp>, [HIL-1602], <sequence-number>, FFDC, CRITICAL, <system-name>, Multiple temperature sensors failed. Service immediately.`

Probable Cause Indicates that temperature readings from multiple sensors are out of range.

Recommended Action Run the **fanShow** command to verify that all fans are operating correctly. Replace any deteriorating fan field-replaceable units (FRUs).

Run the **tempShow** command to verify temperature values. If any sensor is too high, monitor the switch. Try rebooting or power cycling the switch.

Severity CRITICAL

HIL-1603

Message `<timestamp>, [HIL-1603], <sequence-number>, FFDC, CRITICAL, <system-name>, <failure count> fans out of service. System is shutting down immediately.`

Probable Cause Indicates that the total fan failure count is greater than or equal to two.

Recommended Action To avoid causing damage to the switch, the system shuts down automatically. To help prevent future problems, make sure that all the fans are working properly.

Severity CRITICAL

HIL-1605

Message `<timestamp>, [HIL-1605], <sequence-number>, FFDC, INFO, <system-name>, High temperature (<measured temperature> C), fan speed increasing per environmental specifications.`

Probable Cause Indicates that temperatures in the system have risen above the threshold and that the fan speed is being increased.

Recommended Action No action required.

Severity INFO

HIL-1610

Message `<timestamp>, [HIL-1610], <sequence-number>, FFDC, WARNING, <system-name>, Fan/PS unit <Combo fan/power supply unit number> not supplying power, fan speeds not available. Please ensure that the unit has power and the switch is on.`

Probable Cause Indicates that the power supply is not connected to a power source or it is not switched on or the unit is faulty. Applicable only to Brocade 5100.

Recommended Action Ensure that the power cord is connected to the unit with a valid power source and then switch on the unit. If the problem persists, try reseating the unit. If the problem still persists replace the FRU.

Severity WARNING

HIL-1650

Message `<timestamp>, [HIL-1650], <sequence-number>, ERROR, <system-name>, <failure count> unable to detect both WWN cards in chassis. Access to WWN halted.`

Probable Cause One or both of the WWN cards is missing. Both WWN cards must be present for normal operation.

Recommended Action Make sure both WWN cards are inserted.

Severity ERROR

Chapter

HLO System Messages

46

HLO-1001

Message `<timestamp>, [HLO-1001], <sequence-number>, FFDC, ERROR, <system-name>, Incompatible Inactivity timeout <dead timeout> from port <port number>, correct value <value>.`

Probable Cause Indicates that the HLO message was incompatible with the value specified in the FSPF protocol. The Brocade switch will not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO dead timeout value is not configurable, so this error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action The dead timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

Severity ERROR

HLO-1002

Message `<timestamp>, [HLO-1002], <sequence-number>, FFDC, ERROR, <system-name>, Incompatible Hello timeout <HLO timeout> from port <port number>, correct value <correct value>.`

Probable Cause Indicates that the HLO message was incompatible with the value specified in the FSPF protocol. The Brocade switch will not accept FSPF frames from the remote switch.

In the Fabric OS, the HLO timeout value is not configurable, so this error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action The HLO timeout value of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

Severity ERROR

HLO-1003

Message `<timestamp>, [HLO-1003], <sequence-number>, FFDC, ERROR, <system-name>, Invalid Hello received from port <port number>, Domain = <domain ID>, Remote Port =<remote port ID>.`

Probable Cause Indicates that the HLO message received was invalid and the frame was dropped. The Brocade switch will not accept FSPF frames from the remote switch.

The switch has received an invalid HLO because either the domain or port number in the HLO message has an invalid value. This error can only occur when the Brocade switch is connected to a switch from another manufacturer.

Recommended Action The HLO message of the remote switch must be compatible with the value specified in the FSPF protocol. Refer to the documentation for the other manufacturer's switch to change this value.

Severity ERROR

Severity ERROR

Chapter

HMON System Messages

47

HMON-1001

Message `<timestamp>, [HMON-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, <Failure description>`

Probable Cause Indicates there was a problem reading an essential file containing configuration information from the nonvolatile storage device. This could be the result of a missing file or a corrupt file system.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware to your switch.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

Chapter

HSL System Messages

48

HSL-1000

Message `<timestamp>, [HSL-1000], <sequence-number>,, CRITICAL, <system-name>, HSL initialization failed.`

Probable Cause Indicates an HSL initialization failure.

Recommended Action No action is required.

Severity CRITICAL

HSL-1001

Message `<timestamp>, [HSL-1001], <sequence-number>,, CRITICAL, <system-name>, Failed to acquire system mac address pool.`

Probable Cause Indicates the failure to acquire a system address.

Recommended Action No action is required.

Severity CRITICAL

HSL-1002

Message `<timestamp>, [HSL-1002], <sequence-number>,, INFO, <system-name>, SFP for interface <Interface name> is inserted.`

Probable Cause Indicates an SFP is inserted.

Recommended Action No action is required.

Severity INFO

HSL-1003

Message `<timestamp>, [HSL-1003], <sequence-number>,, INFO, <system-name>, SFP for interface <Interface name> is removed.`

Probable Cause Indicates an SFP is removed.

Recommended Action No action is required.

Severity INFO

HSL-1004

Message `<timestamp>, [HSL-1004], <sequence-number>,, ERROR, <system-name>, Incompatible SFP for interface <Interface name> is detected.`

Probable Cause Indicates an incompatible SFP for the interface has been inserted.

Recommended Action Use the correct SFP for this interface.

Severity ERROR

HSL-1004

Message `<timestamp>, [HSL-1004], <sequence-number>,, ERROR, <system-name>, Incompatible SFP for interface <Interface name> is detected.`

Probable Cause Indicates an incompatible SFP for the interface has been inserted.

Recommended Action Use the correct SFP for this interface.

Severity ERROR

HSL-1005

Message `<timestamp>, [HSL-1005], <sequence-number>,, CRITICAL, <system-name>, Failed to initialize with FSS.`

Probable Cause Indicates a failure to initialize the FSS.

Recommended Action No action is required.

Severity CRITICAL

HSL-1006

Message `<timestamp>, [HSL-1006], <sequence-number>,, CRITICAL, <system-name>, Failed to get kernel page size <PageSize> bytes for mmap.`

Probable Cause Indicates that there is not enough contiguous kernel memory.

Recommended Action Install more memory on board.

Severity CRITICAL

HSL-1007

Message `<timestamp>, [HSL-1007], <sequence-number>,, ERROR, <system-name>, Failed to read SFP for interface <InterfaceName>.`

Probable Cause Indicates a failure to read an SFP.

Recommended Action No action is required.

Severity ERROR

Chapter

HTTP System Messages

49

HTTP-1001

Message `<timestamp>, [HTTP-1001], <sequence-number>,, INFO, <system-name>, Switch PIDformat has changed to <current PID format>.`

Probable Cause Indicates that the PID format was changed by the administrator.

Recommended Action No action is required. For more information on PID format, refer to the *Fabric OS Administrator's Guide*.

Severity INFO

HTTP-1002

Message `<timestamp>, [HTTP-1002], <sequence-number>, AUDIT, INFO, <system-name>, Zoning transaction initiated by User: <User Name>, Role: <User Role> completed successfully.`

Probable Cause Indicates that the zoning database has been changed.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

HTTP-1003

Message `<timestamp>, [HTTP-1003], <sequence-number>, AUDIT, INFO, <system-name>, Zoning transaction initiated by User: <User Name>, Role: <User Role> could not be completed successfully - <Reason Message>.`

Probable Cause Indicates an error in completing the zoning transaction.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

49 HTTP-1003

Chapter

IBD System Messages

50

IBD-1001

Message `<timestamp>, [IBD-1001], <sequence-number>,, ERROR, <system-name>, Slot <slot number>, Port GE<port number>:  Maximum attempts to restart failed. Disabling port.`

Probable Cause Indicates that the specified port has crashed unexpectedly and restarting attempts have failed.

Recommended Action Power off and power on the blade using the **slotPowerOff** and **slotPowerOn** commands.

Severity ERROR

Chapter

IBPD System Messages

51

IBPD-1001

Message `<timestamp>, [IBPD-1001], <sequence-number>,, WARNING, <system-name>, <Function name>:<Line number> initiator name length exceeds the <Max length limit> character limit [<Initiator name>]`

Probable Cause Indicates that the initiator name length exceeds the supported limit of characters.

Recommended Action Change the initiator name, keeping the number of characters within the supported limit.

Severity WARNING

IBPD-1002

Message `<timestamp>, [IBPD-1002], <sequence-number>,, WARNING, <system-name>, <Function name>:<Line number> target name length exceeds the <Max length limit> character limit [<target name>]`

Probable Cause Indicates that the target name length exceeds the supported limit.

Recommended Action Redo the discovery to get the latest target list, and try again.

Severity WARNING

IBPD-1003

Message `<timestamp>, [IBPD-1003], <sequence-number>,, WARNING, <system-name>, iSCSI login sessions exceed the maximum limit at slot <Slot number> port ge<Port number>`

Probable Cause Indicates that the iSCSI login sessions exceed the supported limit per port.

Recommended Action Use another port to log in.

Severity WARNING

51 IBPD-1003

Chapter

ICPD System Messages

52

ICPD-1001

Message `<timestamp>, [ICPD-1001], <sequence-number>,, ERROR, <system-name>, Failed to allocate memory: (<function name>).`

Probable Cause Indicates that the specified function failed to allocate memory.

Recommended Action Check memory usage on the switch using the **memShow** command.

Reboot or power cycle the switch.

Severity ERROR

ICPD-1002

Message `<timestamp>, [ICPD-1002], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module> rc = <error>.`

Probable Cause Indicates that an initialization of a module within the ICPD failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference* for more information on this command.

Severity ERROR

ICPD-1003

Message `<timestamp>, [ICPD-1003], <sequence-number>,, INFO, <system-name>, iSCSI configuration has been committed by switch (<domain id>).`

Probable Cause Indicates the iSCSI configuration has been committed by a remote switch in the fabric.

Recommended Action No action is required.

Severity INFO

ICPD-1004

Message `<timestamp>, [ICPD-1004], <sequence-number>,, WARNING, <system-name>, iSNS Client service is detected on multiple switches in fabric.`

Probable Cause Indicates the iSNS Client service is enabled on multiple switches in the fabric.

Recommended Action Enable the iSNS Client service on a single switch in the fabric using the **fosConfig** command. Refer to the *Fabric OS Command Reference* for more information on this command.

Severity WARNING

ICPD-1005

Message `<timestamp>, [ICPD-1005], <sequence-number>,, WARNING, <system-name>, iSCSI configuration between local switch (<local domain id>) and peer (<peer domain id>) is out of sync. iSCSI login is not allowed.`

Probable Cause Indicates that iSCSI switches in the fabric have different configurations in AUTH, VT, or DD.

Recommended Action Synchronize the configuration in the fabric using the **iscsiCfg** command. Refer to the *Fabric OS Command Reference* for more information on this command.

Severity WARNING

ICPD-1006

Message `<timestamp>, [ICPD-1006], <sequence-number>,, INFO, <system-name>, iSCSI service is <status> on the switch.`

Probable Cause Indicates the iSCSI service is enabled or disabled on the switch.

Recommended Action No action is required.

Severity INFO

ICPD-1007

Message `<timestamp>, [ICPD-1007], <sequence-number>,, INFO, <system-name>, iSNSC service is <status> on the switch.`

Probable Cause Indicates the iSNSC service is enabled or disabled on the switch.

Recommended Action No action is required.

Severity INFO

ICPD-1008

Message `<timestamp>, [ICPD-1008], <sequence-number>,, INFO, <system-name>, iSCSI switch (<domain id>) is <status>.`

Probable Cause Indicates the iSCSI switch is reachable or unreachable.

Recommended Action No action is required.

Severity INFO

Chapter

IPAD System Messages

53

IPAD-1000

Message

```
<timestamp>, [IPAD-1000], <sequence-number>,, INFO, <system-name> <Type of
managed entity> <Instance number of managed entity> <Type of network interface>
<Instance number of network interface> <Protocol address family> <Source of
address change> <Value of address and prefix> <DHCP enabled or not>.
```

Probable Cause Indicates that a change in the local IP address has occurred. If the source of the address change is manual, this means that the address change was initiated by a user. If the source of the address change is the dynamic host configuration protocol (DHCP), this means that the address change resulted from interaction with a DHCP server.

Recommended Action No action is required.

Severity INFO

IPAD-1001

Message

```
<timestamp>, [IPAD-1001], <sequence-number>,, INFO, <system-name> <Type of
managed entity> <Instance number of managed entity> <Protocol address family>
<Source of address change> <Value of addres> <DHCP enabled or not>.
```

Probable Cause Indicates that a change in the gateway IP address has occurred. If the source of the address change is manual, this means that the address change was initiated by a user. If the source of the address change is the dynamic host configuration protocol (DHCP), this means that the address change resulted from interaction with a DHCP server.

Recommended Action No action is required.

Severity INFO

Chapter

IPS System Messages

54

IPS-1001

Message `<timestamp>, [IPS-1001], <sequence-number>,, WARNING, <system-name>, <message> FCIP License Not Installed (<error>)`

Probable Cause Indicates that the FCIP license is not installed on the switch.

Recommended Action Run the **licenseShow** command to check the installed licenses on the switch. Contact your switch supplier for a FCIP license. Run the **licenseAdd** command to add the license to your switch.

Severity WARNING

IPS-1002

Message `<timestamp>, [IPS-1002], <sequence-number>,, ERROR, <system-name>, Failed to initialize <module> rc = <error>`

Probable Cause Indicates that an initialization of a module within the IPS daemon failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

IPS-1003

Message `<timestamp>, [IPS-1003], <sequence-number>,, WARNING, <system-name>, <function name>(): Failed to allocate memory while performing <message>`

Probable Cause Indicates that memory resources are low. This might be a transient problem.

Recommended Action If the message persists, check the memory usage on the switch, using the **memShow** command.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

IPS-1004

Message `<timestamp>, [IPS-1004], <sequence-number>,, WARNING, <system-name>, Port Config Mode Mismatch slot (<slot>) port(ge<port>): current mode is (<current mode>)`

Probable Cause Indicates that configured Port Mode is different from the intended use.

Recommended Action Change the port configuration (by deleting configured FCIP tunnels or iSCSI sessions) to return the port mode to neutral before attempting to configure the port for a different mode or use.

Severity WARNING

IPS-1005

Message

```
<timestamp>, [IPS-1005], <sequence-number>,, WARNING, <system-name>, Tunnel
Authorization Failure for slot (<slot>) port(ge<port>) tunnel ID(<tunnel number>)
reason (<reason>)
```

Probable Cause Indicates that tunnel setup failed because of an authorization failure from the remote side. A reason for such a failure could be a WWN mismatch.

Recommended Action Change the tunnel configuration on one side of the tunnel to authorize the remote side to set up the tunnel.

Severity WARNING

IPS-1006

Message

```
<timestamp>, [IPS-1006], <sequence-number>,, WARNING, <system-name>, Tunnel
Configuration Mismatch for slot (<slot>) port(<port>) tunnel ID(<tunnel number>)
reason (<reason>)
```

Probable Cause Indicates that tunnel setup failed because of a configuration mismatch between the two ends. The reason for such a mismatch could be a Compression setting or WanTOV enforcement.

Recommended Action Change the tunnel configuration on one side of the tunnel to match that of the other side to set up the tunnel.

Severity WARNING

Chapter

ISCS System Messages

55

ISCS-1000

Message `<timestamp>, [ISCS-1000], <sequence-number>,, ERROR, <system-name>, Slot <slot number> Port GE<port number> crashed unexpectedly.`

Probable Cause Indicates the specified port has crashed.

Recommended Action No action is required; the port will restart automatically.

Severity ERROR

Chapter

ISNS System Messages

56

ISNS-1001

Message `<timestamp>, [ISNS-1001], <sequence-number>,, INFO, <system-name>, Configuration peering with external iSNS server <New config iSNS server IP address> slot/port <New config Slot number>/ge<New config port number> (current <Current iSNS server IP address> <Current slot number>/ge<Current port number>).`

Probable Cause Indicates that the user has issued the **isnscCfg** command.

Recommended Action No action is required.

Severity INFO

ISNS-1002

Message `<timestamp>, [ISNS-1002], <sequence-number>,, INFO, <system-name>, Start peering with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.`

Probable Cause Indicates that peering has started with the specified external internet storage name service (iSNS) server.

Recommended Action No action is required.

Severity INFO

ISNS-1003

Message `<timestamp>, [ISNS-1003], <sequence-number>,, INFO, <system-name>, Peering with external iSNS server is disabled.`

Probable Cause Indicates the IP address of the internet storage name service (iSNS) server is zero. Hence peering is disabled.

Recommended Action If you wish to enable the iSNS server, use the **isnscCfg** command to show or set the server IP address; otherwise, no action is required.

Severity INFO

ISNS-1004

Message `<timestamp>, [ISNS-1004], <sequence-number>,, WARNING, <system-name>, Timeout refreshing iSNS database with iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number> Reg-Period <Registration-Period in seconds>.`

Probable Cause Indicates that the internet storage name service (iSNS) client failed to receive a successful response for a **DevAttrQry** within the specified *Registration-Period*.

Recommended Action Verify the connection of the iSNS server to the slot or port.

Severity WARNING

ISNS-1005

Message `<timestamp>, [ISNS-1005], <sequence-number>,, INFO, <system-name>, User request re-register with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.`

Probable Cause Indicates a user has requested a re-register with the specified external internet storage name service (iSNS) server.

Recommended Action No action is required.

Severity INFO

ISNS-1006

Message `<timestamp>, [ISNS-1006], <sequence-number>,, INFO, <system-name>, Start re-register with external iSNS server <iSNS server IP address> slot/port <Slot number>/ge<Port number>.`

Probable Cause Indicates that the re-register with the specified external internet storage name service (iSNS) server has started.

Recommended Action No action is required.

Severity INFO

ISNS-1008

Message `<timestamp>, [ISNS-1008], <sequence-number>,, INFO, <system-name>, Peering with external iSNS server <iSNS server IP address> not started because configuration unchanged.`

Probable Cause Indicates that peering with the external internet storage name service (iSNS) server was already started with the same configuration.

Recommended Action No action is required. You may change the configuration and retry the peering with the external iSNS server.

Severity INFO

ISNS-1009

Message `<timestamp>, [ISNS-1009], <sequence-number>,, INFO, <system-name>, Peering with external iSNS server <iSNS server IP address> not started because no virtual targets found.`

Probable Cause Indicates that no virtual targets were found, so peering was not started.

Recommended Action No action is required. Peering will resume automatically when virtual targets are detected.

Severity INFO

ISNS-1010

Message `<timestamp>, [ISNS-1010], <sequence-number>,, WARNING, <system-name>, Slot/port <Slot>/ge<Port> is out of range.`

Probable Cause Indicates the slot or port is out of range.

Recommended Action Retry with a valid slot or port. Refer to the appropriate hardware reference manual for valid slot and port ranges.

Severity WARNING

ISNS-1011

Message `<timestamp>, [ISNS-1011], <sequence-number>,, INFO, <system-name>, iSNS Client Service is <iSNS client State (enabled/disabled)>.`

Probable Cause Indicates the current state of the internet storage name services (iSNS) client is either enabled or disabled.

Recommended Action No action is required. Use the **fosConfig** command to display, enable, or disable the iSNS client service.

Severity INFO

ISNS-1013

Message `<timestamp>, [ISNS-1013], <sequence-number>,, WARNING, <system-name>, iSNS server connection failure.`

Probable Cause Indicates that the internet storage name service (iSNS) client failed to establish a connection with the iSNS server.

Recommended Action Verify the connection of the iSNS server to the slot or port. Use the **isnscCfg** command to display or correct the server IP address.

Severity WARNING

ISNS-1014

Message `<timestamp>, [ISNS-1014], <sequence-number>,, INFO, <system-name>, Start peering with external iSNS server <iSNS server IP address> on management port.`

Probable Cause Indicates that peering has started with the specified external internet storage name service (iSNS) on the management port.

Recommended Action No action is required.

Severity INFO

Chapter

KAC System Messages

57

KAC-1002

Message `<timestamp>, [KAC-1002], <sequence-number>,, ERROR, <system-name>, KAC(<Key Vault Type>) communication Error: Error connecting to <Backup or Primary>.`

Probable Cause Indicates that the key archival client is unable to communicate with the *primary* or *backup* key vault.

Recommended Action Determine whether the configured key vault is operational, and if it is not, change the switch key vault settings or resolve the operational problem at the vault.

Severity ERROR

KAC-1004

Message `<timestamp>, [KAC-1004], <sequence-number>,, ERROR, <system-name>, KAC <Operation Description> to key vault failed.`

Probable Cause Indicates that the key archival client is unable to do a certain operation to the *primary* or *backup* key vault.

Recommended Action Determine whether the configured key value is operational, and if it is not, change the switch key vault settings or resolve the operational problem at the vault.

Severity ERROR

KAC-1006

Message `<timestamp>, [KAC-1006], <sequence-number>,, ERROR, <system-name>, Switch to key vault trustee link was not established.`

Probable Cause Indicates that the trustee link between the switch and the key vault was not established.

Recommended Action Establish a trustee link between the switch and the key vault.

Severity ERROR

KAC-1007

Message `<timestamp>, [KAC-1007], <sequence-number>,, ERROR, <system-name>, KAC put key to key vault failed, LUN=<LUN Number>, keyID=<Key ID Value>, errno=<Error Number>.`

Probable Cause Indicates that the key archival client is unable to put to the *primary* or *backup* key vault.

Recommended Action Determine whether the configured key value is operational, and if it is not, change the switch key vault settings or resolve the operational problem at the vault.

Severity ERROR

KAC-1008

Message `<timestamp>, [KAC-1008], <sequence-number>,, ERROR, <system-name>, Putting TEP failed check if there is already an unapproved TEP then delete it, RC=<Error code from lkm>.`

Probable Cause Indicates that there was already a pending unapproved TEP at the LKM.

Recommended Action Log in to the LKM and delete the unapproved TEP.

Severity ERROR

KAC-1009

Message `<timestamp>, [KAC-1009], <sequence-number>,, ERROR, <system-name>, Primary(<Primary Keyvault IP Address>) and secondary(<Secondary Keyvault IP Address>) keyvaults are not in sync. Detected key mismatch with KeyID = <KeyID>.`

Probable Cause Indicates that primary and secondary contents are not synchronized.

Recommended Action Synchronize the contents of the primary and secondary using instructions provided by the provider.

Severity ERROR

Chapter

KSWD System Messages

58

KSWD-1001

Message `<timestamp>, [KSWD-1001], <sequence-number>, FFDC, WARNING, <system-name>, <Software component>:<Software component Process ID> failed to refresh (<Current time>:<Refresh time>).`

Probable Cause Indicates that one of the critical daemons is found to be nonresponsive. An abort signal is sent.

Recommended Action Copy the warning message along with any core file information, and contact your switch service provider.

Severity WARNING

KSWD-1002

Message `<timestamp>, [KSWD-1002], <sequence-number>, FFDC, WARNING, <system-name>, Detected termination of process <Software component>:<Software component Process ID>.`

Probable Cause Indicates a process on the switch has ended unexpectedly.

Recommended Action Copy the warning message along with any core file information, and contact your switch service provider.

Severity WARNING

Chapter

KTRC System Messages

59

KTRC-1001

Message `<timestamp>, [KTRC-1001], <sequence-number>,, WARNING, <system-name>, Dump memory size exceeds dump file size`

Probable Cause Indicates the dump memory size has exceeded the dump file size.

Recommended Action No action is required.

Severity WARNING

KTRC-1002

Message `<timestamp>, [KTRC-1002], <sequence-number>,, INFO, <system-name>, Concurrent trace dumping.`

Probable Cause Indicates the initial background dump has not completed.

Recommended Action No action is required.

Severity INFO

KTRC-1003

Message `<timestamp>, [KTRC-1003], <sequence-number>,, ERROR, <system-name>, Cannot open ATA dump device`

Probable Cause Indicates the ATA dump driver is not initialized properly.

Recommended Action No action is required.

Severity ERROR

KTRC-1004

Message `<timestamp>, [KTRC-1004], <sequence-number>,, ERROR, <system-name>, Cannot write to ATA dump device`

Probable Cause Indicates the write boundary in the ATA dump device has exceeded.

Recommended Action No action is required.

Severity ERROR

KTRC-1005

Message `<timestamp>, [KTRC-1005], <sequence-number>,, ERROR, <system-name>, Trace initialization failed. <Reason initialization failed>. <Internal error code>.`

Probable Cause Indicates that a trace was unable to initialize.

Recommended Action No action is required.

Severity ERROR

Chapter

L2SYS System Messages

60

L2SS-1001

Message `<timestamp>, [L2SS-1001], <sequence-number>,, ERROR, <system-name>, Socket Error: <reason> for socket <sockname>  the error code <errorname>.`

Probable Cause Indicates an error has occurred in the Linux socket.

Recommended Action Restart the l2ssd daemon.

Severity ERROR

L2SS-1002

Message `<timestamp>, [L2SS-1002], <sequence-number>,, ERROR, <system-name>, Initialization error: <reason>.`

Probable Cause Indicates that the l2sys encountered an error during initialization.

Recommended Action Restart the l2sysd daemon.

Severity ERROR

L2SS-1003

Message `<timestamp>, [L2SS-1003], <sequence-number>,, ERROR, <system-name>, Message Queue Error : Message queue create failed.`

Probable Cause Indicates that the l2sys encountered with System Service Manager (SSM) message queue errors.

Recommended Action Restart the l2sysd daemon.

Severity ERROR

L2SS-1004

Message `<timestamp>, [L2SS-1004], <sequence-number>,, ERROR, <system-name>, FDB error: Error in creating AVL tree.`

Probable Cause Indicates that the l2sys has encountered an error while initializing the AVL tree.

Recommended Action Restart the l2sysd daemon.

Severity ERROR

L2SS-1005

Message `<timestamp>, [L2SS-1005], <sequence-number>,, ERROR, <system-name>, Mac-address-table hash failed even after two attempts for slot <slot> chip <chip>.`

Probable Cause Indicates a mac-address-table hash failure happened even after two hash changes on the chip.

Recommended Action Restart the l2sysd daemon.

Severity ERROR

L2SS-1006

Message `<timestamp>, [L2SS-1006], <sequence-number>,, INFO, <system-name>, Mac-address-table table on slot <slot_id> chip <chip_id> is 95 percent full.`

Probable Cause Indicates that the mac-address-table on the chip is 95% full.

Recommended Action Clear some of the entries, or wait till old entries age out.

Severity INFO

L2SS-1007

Message `<timestamp>, [L2SS-1007], <sequence-number>,, INFO, <system-name>, MMac-address-table on slot <slot_id> chip <chip_id> is less than 90 percent full.`

Probable Cause Indicates that the mac-address-table is less than 90% full.

Recommended Action No action is required. L2SYS will start learning the entries.

Severity INFO

Chapter

LACP System Messages

61

LACP-1001

Message `<timestamp>, [LACP-1001], <sequence-number>,, ERROR, <system-name>, <module> Error opening socket (<error>).`

Probable Cause Indicates that the initialization of a module within the LACP daemon has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

Chapter

LANCE System Messages

62

LANCE-1000

Message `<timestamp>, [LANCE-1000], <sequence-number>,, ERROR, <system-name>, Slot <slot number> Port GE <port number>:  Maximum attempts to restart failed. Disabling port.`

Probable Cause Indicates that the port is disabled.

Recommended Action No action is required.

Severity ERROR

Chapter

LFM System Messages

63

LFM-1001

Message `<timestamp>, [LFM-1001], <sequence-number>,, INFO, <system-name>, The Logical Fabric Manager service is disabled.`

Probable Cause Indicates that the Logical Fabric Manager service is disabled. Note that the Logical Fabric Manager service is enabled by the factory setting and it is not user configurable.

Recommended Action No action is required.

Severity INFO

LFM-1002

Message `<timestamp>, [LFM-1002], <sequence-number>,, INFO, <system-name>, The Logical Fabric Manager service is enabled.`

Probable Cause Indicates that the Logical Fabric Manager service is enabled. Note that the Logical Fabric Manager service is enabled by the factory setting and it is not user configurable.

Recommended Action No action is required.

Severity INFO

LFM-1003

Message `<timestamp>, [LFM-1003], <sequence-number>,, INFO, <system-name>, The Logical Fabric Manager configuration is set to default.`

Probable Cause Indicates that the Logical Fabric Manager configuration is set to default. This will remove all prior Logical Fabric Manager configurations. This operation is not supported, currently.

Recommended Action No action is required.

Severity INFO

LFM-1004

Message `<timestamp>, [LFM-1004], <sequence-number>,FFDC, CRITICAL, <system-name>, HA is out of sync for opcode <HA OPCODE>, error value <error value>.`

Probable Cause Indicates the trigger for some internal logging purpose.

Recommended Action Send the ffdc log to the support.

Severity CRITICAL

LFM-1005

Message `<timestamp>, [LFM-1005], <sequence-number>,, WARNING, <system-name>, Logical port <portnum> disabled with reason <portnum>(<reason>).`

Probable Cause Indicates the trigger for logical port disable for internal logging purpose.

Recommended Action This could be due to a port segmentation. Check the reason for the port disable using the **switchshow** command. Rectify the disable based on the reason.

Severity WARNING

LFM-1006

Message `<timestamp>, [LFM-1006], <sequence-number>,, WARNING, <system-name>, The switch with domain <domain> with firmware version <version> has joined the FID <FID> fabric and may not be compatible with XISL use.`

Probable Cause Indicates that validation of firmware compatibility for XISL use on the specified switch has failed.

Recommended Action Check release notes to verify if this firmware is compatible with XISL use. If it is not switch should be removed from the fabric.

Severity WARNING

Chapter

LOG System Messages

64

LOG-1000

Message `<timestamp>, [LOG-1000], <sequence-number>,, INFO, <system-name>, Previous message repeated <repeat count> times`

Probable Cause Indicates the previous message repeated the specified number of times.

Recommended Action No action is required.

Severity INFO

LOG-1001

Message `<timestamp>, [LOG-1001], <sequence-number>, FFDC, WARNING, <system-name>, A log message was dropped`

Probable Cause Indicates a log message was dropped. A trace dump file is created.

Recommended Action Run the **reboot** command for nonbladed switches or the **haFailover** command on bladed switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

LOG-1002

Message `<timestamp>, [LOG-1002], <sequence-number>, FFDC, WARNING, <system-name>, A log message was dropped`

Probable Cause Indicates a message was not recorded by the error logging system. A trace dump file is created. The message might still be visible through SNMP or other management tools.

Recommended Action Run the **reboot** command for nonbladed switches or the **haFailover** command on bladed switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

LOG-1003

Message `<timestamp>, [LOG-1003], <sequence-number>,, INFO, <system-name>, The log has been cleared.`

Probable Cause Indicates the persistent error log has been cleared.

Recommended Action No action is required.

Severity INFO

Chapter

LSDB System Messages

65

LSDB-1001

Message `<timestamp>, [LSDB-1001], <sequence-number>,, ERROR, <system-name>, Link State ID <link state ID> out of range`

Probable Cause Indicates the specified link state database ID is out of the acceptable range. The valid *link state ID* is the same as the valid domain ID, whose range is from 1 through 239. The switch will discard the record because it is not supported.

Recommended Action No action is required.

Severity ERROR

LSDB-1002

Message `<timestamp>, [LSDB-1002], <sequence-number>,, INFO, <system-name>, Local Link State Record reached max incarnation#`

Probable Cause Indicates the local link state database reached the maximum incarnations.

An "incarnation" is a progressive number that identifies the most recent version of the LSR (link state record). The switch generates its local link state record when first enabled. The incarnation number will begin again at 0x80000001 after reaching 0x7FFFFFFF.

Recommended Action No action is required.

Severity INFO

LSDB-1003

Message `<timestamp>, [LSDB-1003], <sequence-number>, FFDC, CRITICAL, <system-name>, No database entry for local Link State Record, domain <local domain>`

Probable Cause Indicates there is no local link state record entry in the link state database. The switch should always generate its own local entry when starting up.

An "incarnation" is a progressive number that identifies the most recent version of the LSR (link state record). The switch generates its local link state record when first enabled. By disabling and enabling the switch, a new local link state record is generated.

Recommended Action Run the **switchDisable** and **switchEnable** commands. A new local link state record is generated during the switch enable.

Severity CRITICAL

LSDB-1004

Message `<timestamp>, [LSDB-1004], <sequence-number>,, WARNING, <system-name>, No Link State Record for domain <local domain>`

Probable Cause Indicates there is no link state record for the specified *local domain*.

Recommended Action No action is required. The other switch will pass the LSD once the fabric is stable.

Severity WARNING

Chapter

MFIC System Messages

66

MFIC-1001

Message `<timestamp>, [MFIC-1001], <sequence-number>,, ERROR, <system-name>, failure at sysmod_scn registry rc= <failure reason>`

Probable Cause Indicates the system is temporarily out of resources.

Recommended Action No action is required; this message is often transitory.

If the message persists, run a switch **reboot** or an **haFailover** command (if applicable).

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

MFIC-1002

Message `<timestamp>, [MFIC-1002], <sequence-number>,, INFO, <system-name>, Chassis FRU header not programmed for switch NID, using defaults (applies only to FICON environments).`

Probable Cause Indicates that custom switch node descriptor (NID) fields have not been programmed in nonvolatile storage. The default values are used. The Switch NID is used only in the following SB ELS frames: Request Node Identification Data (RNID) and Registered Link Incident Record (RLIR).

The use of SB-3 link incident registration and reporting is typically limited to FICON environments.

Recommended Action No action is required if SB-3 link incident registration and reporting is not used by the host or if default values are desired for the switch node descriptor fields.

Severity INFO

MFIC-1003

Message `<timestamp>, [MFIC-1003], <sequence-number>,, WARNING, <system-name>, Effective Insistent domain ID for the fabric changed from <state> to <state>`

Probable Cause Indicates that one or more switches joined the fabric with an insistent domain ID (IDID) mode setting that is different from the current effective IDID mode for the fabric. This message also occurs when the IDID for the fabric has been turned on or off. The possible values for the state are "On" and "Off".

Recommended Action IDID mode is a fabric-wide mode; make sure that any switches added to the fabric are configured with the same IDID mode as the fabric. If you are enabling or disabling IDID mode, this message is for information purposes only, and no action is required.

IDID mode can be set using the **configure** command in the CLI or checking the Advanced Web Tools **Switch Admin > Configure Tab > Fabric Subtab > Insistent Domain ID Mode** check box. The switch must be disabled to change the IDID mode.

Severity WARNING

Chapter

MPTH System Messages

67

MPTH-1001

Message `<timestamp>, [MPTH-1001], <sequence-number>, FFDC, ERROR, <system-name>, Null parent, lsId = <number>`

Probable Cause Indicates a null parent was reported. MPATH uses a tree structure in which the parent is used to connect to the root of the tree.

Recommended Action No action is required.

Severity ERROR

MPTH-1002

Message `<timestamp>, [MPTH-1002], <sequence-number>, FFDC, ERROR, <system-name>, Null lsrP, lsId = <ls ID number>`

Probable Cause Indicates a link state record is null.

Recommended Action No action is required.

Severity ERROR

MPTH-1003

Message `<timestamp>, [MPTH-1003], <sequence-number>,, WARNING, <system-name>, No minimum cost path in candidate list`

Probable Cause Indicates the FSPF module has determined that there is no minimum cost path (MPath) available in the candidate list.

Recommended Action No action is required.

Severity WARNING

67 MPTH-1003

Chapter

MQ System Messages

68

MQ-1004

Message `<timestamp>, [MQ-1004], <sequence-number>,, ERROR, <system-name>, mqRead, queue = <queue name>, queue ID = <queue ID>, type = <message type>`

Probable Cause Indicates an unexpected message has been received in the specified message queue. The *queue name* is always fspf_q. The *queue ID* and corresponding *message type* can be any of the following:

- 2 - MSG_TX
- 3 - MSG_INTR
- 4 - MSG_STR
- 6 - MSG_ASYNC_IU
- 7 - MSG_LINIT_IU
- 8 - MSG_RSCN
- 9 - MSG_IOCTL
- 10 - MSG_ACCEPT
- 11 - MSG_IU_FREE
- 12 - MSG_US
- 13 - MSG_EXT_RSCN
- 14 - MSG_RDTS_START
- 15 - MSG_RDTS_SENDEFP
- 16 - MSG_RDTS_RESET

Recommended Action No action is required.

Severity ERROR

MQ-1005

Message `<timestamp>, [MQ-1005], <sequence-number>,, WARNING, <system-name>, queue <queue name>: queue full (miss=<miss count>)`

Probable Cause Indicates the corresponding message queue is full.

Recommended Action No action is required.

Severity WARNING

MQ-1006

Message `<timestamp>, [MQ-1006], <sequence-number>,, WARNING, <system-name>, queue <queue name>: msg too long (<number of bytes>:<message queue size>)`

Probable Cause Indicates the incoming message size is larger than the message queue size.

Recommended Action No action is required.

Severity WARNING

Chapter

MS System Messages

69

MS-1001

Message

```
<timestamp>, [MS-1001], <sequence-number>,, WARNING, <system-name>, MS Platform
Segmented port=<port number> (<port number (hex)>) (<reason for segmentation>
<domain> (<domain (hex)>))
```

Probable Cause

Indicates the management server (MS) has segmented from another switch *domain* at the specified *port number* because of errors or inconsistencies defined in the MS platform service.

Recommended Action

Restart or power cycle the switch.

Severity

WARNING

MS-1002

Message

```
<timestamp>, [MS-1002], <sequence-number>,, INFO, <system-name>, MS Platform
Service Unstable(<message string><domain number>)
```

Probable Cause

Indicates the management server (MS) platform service is unstable.

The *message string* can be one of the following:

- <No Resp for GCAP from>

  The switch did not respond to a request for a GCAP (MS Get Capabilities) command.

- <GCAP sup but not PL by>

  The GCAP (MS Get Capabilities) is supported but the flag for MS platform service is not set.

- <GCAP Rejected (reason =BUSY) by>

  The GCAP (MS Get Capabilities) is not supported by another switch.

- <Reject EXGPLDB from>

  The request to the exchange platform database was rejected. The remote switch might be busy.

The *domain number* is the target domain that caused the error.

Recommended Action

The recommended actions are as follows:

- <No Resp for GCAP from>
  No action is required.
- <GCAP sup but not PL by>
  Set the flag for the MS Platform Service.

- <GCAP Rejected (reason =BUSY) by>
  Run the **firmwareDownload** command to upgrade the firmware level on the switch to a level that supports RCS. RCS is supported in Fabric OS v2.6, v3.1 and greater, and v4.1 and greater.
- <Reject EXGPLDB from>
  Wait a few minutes and try the command again.

Severity INFO

MS-1003

Message `<timestamp>, [MS-1003], <sequence-number>,, INFO, <system-name>, MS detected Unstable Fabric(<message string><domain number>).`

Probable Cause Indicates the management server (MS) detected an unstable fabric; the command or operation might not be successfully completed. This message is often transitory.

The *message string* can be one of the following:

- <DOMAIN_INVALID for a req from>
  The domain is invalid for a request.
- <No WWN for>
  Unable to acquire the World Wide Name (WWN) for the corresponding domain.

The *domain number* is the target domain that caused error.

Recommended Action The fabric might be reconfiguring, forming, or merging. Wait for a few minutes and retry the operation.

Run the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

MS-1004

Message `<timestamp>, [MS-1004], <sequence-number>,, INFO, <system-name>, MS detected ONLY 1 Domain(d=<domain in local resource>).`

Probable Cause Indicates the management server (MS) detected an unstable count of domains in its own local resource.

Recommended Action This message is often transitory.

The fabric might be reconfiguring, forming, or merging. Wait for a few minutes and retry the operation.

Run the **fabricShow** command or the **secFabricShow** command to verify that the number of domains matches the Management Server known domains.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

MS-1005

Message `<timestamp>, [MS-1005], <sequence-number>,, ERROR, <system-name>, MS Invalid CT Response from d=<domain>`

Probable Cause Indicates the management server (MS) received an invalid common transport (CT) response from the switch *domain*. MS expects either a CT accept IU or a reject IU; the MS received neither response, which violates the Fibre Channel Generic Services (FS-GS) specification.

Recommended Action Check the integrity of the FC switch at the specified domain. It is not sending correct MS information as defined by the FC-GS standard.

Severity ERROR

MS-1006

Message `<timestamp>, [MS-1006], <sequence-number>,, ERROR, <system-name>, MS Unexpected iu_data_sz=<number of bytes>`

Probable Cause Indicates the management server (MS) received an information unit (IU) data of unexpected size. The IU payload and the IU size might be inconsistent with each other or with the command that is currently being processed.

Recommended Action Wait for a few minutes and retry the operation.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

MS-1008

Message `<timestamp>, [MS-1008], <sequence-number>,, ERROR, <system-name>, MS Failure while initializing <action>`

Probable Cause Indicates the management server (MS) failed while initializing the specified *action*.

The following *actions* might be displayed:

- <while writing to ms_els_q>
  MS is unable to write a message to the MS Extended Link Service Queue.
- <while inserting timer to timer list>
  MS is unable to add a timer to a resource.

Recommended Action This message is often transitory.

If the error persists, check the available memory on the switch using the **memShow** command.

Severity ERROR

MS-1009

Message `<timestamp>, [MS-1009], <sequence-number>,, ERROR, <system-name>, RLIR event. Switch Port ID is <port number> (<PID (hex)>). Device Port Tag is <port tag>. <message text>.`

Probable Cause Indicates a registered link incident record (RLIR) has been generated for one of the actions indicated by the <message>.

The following messages will be displayed:

- Exceeded bit error rate threshold
- Loss of signal or synchronization
- Not operational seq. recognized
- Primitive sequence timeout
- Unrecognized link incident

Recommended Action Persistent RLIR incidents are likely the result of SAN hardware problems such as bad cables or small form-factor pluggables (SFPs). It may be necessary to replace hardware if these messages persist.

Severity ERROR

MS-1021

Message `<timestamp>, [MS-1021], <sequence-number>,, ERROR, <system-name>, MS WARMBOOT failure(FSS_MS_WARMINIT failed. Reason=<failure reason>).`

Probable Cause Indicates the Fabric OS state synchronization (FSS) warm recovery failed during the WARM INIT phase of a reboot.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

MS-1022

Message `<timestamp>, [MS-1022], <sequence-number>,, INFO, <system-name>, Management Server Platform Service <Activated or Deactivated>.`

Probable Cause Indicates Management Server Platform Service is being activated or deactivated.

Recommended Action No action is required.

Severity INFO

MS-1023

Message `<timestamp>, [MS-1023], <sequence-number>,, INFO, <system-name>, Management Server Topology Discovery Service <Enabled or Disabled>.`

Probable Cause Indicates Management Server Topology Discovery Service is being enabled or disabled.

Recommended Action No action is required.

Severity INFO

MS-1024

Message `<timestamp>, [MS-1024], <sequence-number>,, INFO, <system-name>, Management Server Access Control List is Updated.`

Probable Cause Indicates the management server (MS) Access Control List is saved to non-volatile storage.

Recommended Action No action is required.

Severity INFO

MS-1025

Message `<timestamp>, [MS-1025], <sequence-number>,, WARNING, <system-name>, Possible Failover could have occurred while enabling MS Platform Service.`

Probable Cause Indicates that while the MS Platform Service was being enabled, a failover has occurred. This can leave the fabric in an inconsistent state.

Recommended Action If there is an inconsistency in the Platform service within the fabric, enable the Platform service.

Severity WARNING

MS-1026

Message `<timestamp>, [MS-1026], <sequence-number>,, WARNING, <system-name>, MS Platform disabled port <port number> domain <domain> to block enabling Platform service through merge operation.`

Probable Cause Indicates the management server (MS) has disabled E-port *port number* connected to domain *domain* because implicit enable operation of platform service is blocked.

Recommended Action Enable Platform service on the switch and renable the port to join the fabric.

Severity WARNING

Chapter

MSTP System Messages

70

MSTP-1001

Message `<timestamp>, [MSTP-1001], <sequence-number>,, ERROR, <system-name>, <msg>:<msg>.`

Probable Cause Indicates that the system has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **memShow** command.

Restart or power cycle the switch.

Severity ERROR

MSTP-1002

Message `<timestamp>, [MSTP-1002], <sequence-number>,, ERROR, <system-name>, <msg>:<msg>.`

Probable Cause Indicates that the system has failed to initialize.

Recommended Action Restart or power cycle the switch.

Severity ERROR

MSTP-1003

Message `<timestamp>, [MSTP-1003], <sequence-number>,, ERROR, <system-name>, <msg>:<msg>.`

Probable Cause Indicates a socket connection or socket transferring or receiving error.

Recommended Action If this is a bladed switch, execute the **haFailover** command. If the problem persists or if this is a nonbladed switch, download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

MSTP-2001

Message `<timestamp>, [MSTP-2001], <sequence-number>,, INFO, <system-name>, <msg>`

Probable Cause Indicates that the MSTP bridge mode has changed.

Recommended Action No action is required

Severity INFO

MSTP-2002

Message `<timestamp>, [MSTP-2002], <sequence-number>,, INFO, <system-name>, <Bridge mode information>. My Bridge ID: <Bridge ID> Old Root: <Old Root id> New Root: <New Root ID>`

Probable Cause Indicates that the MSTP bridge or bridge instance root has changed.

Recommended Action No action is required.

Severity INFO

MSTP-2003

Message `<timestamp>, [MSTP-2003], <sequence-number>,, INFO, <system-name>, MSTP instance <instance> is created.`

Probable Cause Indicates that the MSTP instance has created.

Recommended Action No action is required.

Severity INFO

MSTP-2004

Message `<timestamp>, [MSTP-2004], <sequence-number>,, INFO, <system-name>, MSTP instance <instance> is deleted.`

Probable Cause Indicates that the MSTP instance has deleted.

Recommended Action No action is required.

Severity INFO

MSTP-2005

Message `<timestamp>, [MSTP-2005], <sequence-number>,, INFO, <system-name>, Vlan <vlan_ids> is <action> on MSTP instance <instance>.`

Probable Cause Indicates that the MSTP instance has modified.

Recommended Action No action is required.

Severity INFO

MSTP-2006

Message `<timestamp>, [MSTP-2006], <sequence-number>,, INFO, <system-name>, MSTP instance <instance> brigde priority is changed from <priority_old> to <priority_new>.`

Probable Cause Indicates that the MSTP instance priority has modified.

Recommended Action No action is required.

Severity INFO

Chapter

NBFS System Messages

71

NBFS-1001

Message

```
<timestamp>, [NBFS-1001], <sequence-number>,, INFO, <system-name>, Duplicate
E_Port SCN from port <portnumber> in state <state change name> (<state change
number>)
```

Probable Cause

Indicates a duplicate E_Port State Change Number was reported. The neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended Action

No action is required.

Severity

INFO

NBFS-1002

Message

```
<timestamp>, [NBFS-1002], <sequence-number>, FFDC, ERROR, <system-name>, Wrong
input: <state name> to neighbor FSM, state <current state name>, port <portnumber>
```

Probable Cause

Indicates the wrong input was sent to the neighbor finite state machine (NBFSM). NBFSM states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

If this error occurs repeatedly, then there is a problem in the protocol implementation between two switches.

Recommended Action

Run the **nbrStateShow** command to check the neighbor state of the port listed in the message. If it is FULL, then this message can safely be ignored. Otherwise, run the **portDisable** and **portEnable** commands to refresh the port.

Severity ERROR

NBFS-1003

Message `<timestamp>, [NBFS-1003], <sequence-number>,, WARNING, <system-name>, DB_XMIT_SET flag not set in state <current state name>, input <state name>, port <portnumber>`

Probable Cause Indicates the database transmit set flag was not set for the specified input state on the specified port. Neighbor finite state machine (NBFSM) states are as follows:

- 0 - Down
- 1 - Init
- 2 - Database Exchange
- 3 - Database Acknowledge Wait
- 4 - Database Wait
- 5 - Full

Recommended Action No action is required. The Fabric OS automatically recovers from this problem.

Severity WARNING

Chapter

NS System Messages

72

NS-1001

Message `<timestamp>, [NS-1001], <sequence-number>,, WARNING, <system-name>, The response for request 0x<CT command code> from remote switch 0x<Domain Id> is larger than the max frame size the remote switch can support!`

Probable Cause Indicates the response payload exceeds the maximum frame size the remote switch can handle.

Recommended Action Run the **firmwareDownload** command to upgrade the remote switch with firmware v4.3 or higher, or v3.2 or higher, as appropriate for the switch type, so that it can support GMI to handle frame fragmentation and reassembly.

You can also reduce the number of devices connected to the local switch.

Severity WARNING

NS-1002

Message `<timestamp>, [NS-1002], <sequence-number>,, WARNING, <system-name>, Remote switch 0x<Domain Id> has firmware revision lower than 2.2: <Firmware Revision 1st character><Firmware Revision 2nd character><Firmware Revision 3rd character><Firmware Revision 4th character> which is not supported!`

Probable Cause Indicates the local switch cannot interact with the remote switch because of incompatible or obsolete firmware.

Recommended Action Run the **firmwareDownload** command to upgrade the remote switch to the latest level of firmware.

Severity WARNING

NS-1003

Message `<timestamp>, [NS-1003], <sequence-number>,, INFO, <system-name>, Number of local devices <Current local device count>, exceeds the standby can support <Local device count that standby can support>, can't send update.`

Probable Cause Indicates the name server on the standby CP has lower supported capability than the active CP because of different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

Recommended Action To avoid disruption of traffic in the event of an unplanned failover, schedule a firmwareDownload so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the lowest version of firmware.

Severity INFO

NS-1004

Message `<timestamp>, [NS-1004], <sequence-number>,, INFO, <system-name>, Number of local devices <Current local device count>, exceeds the standby can support <Local device count that standby can support>, can't sync.`

Probable Cause Indicates the name server on the standby CP has lower supported capability than the active CP because of different firmware versions running on the active and standby CPs. This means that the active and standby CPs are out of sync. Any execution of the **haFailover** or **firmwareDownload** commands will be disruptive.

Recommended Action To avoid disruption of traffic in the event of an unplanned failover, schedule a **firmwareDownload** so that the active and standby CPs have the same firmware version.

Reduce the local device count to follow the capability of the lowest version of firmware.

Severity INFO

NS-1005

Message `<timestamp>, [NS-1005], <sequence-number>,, WARNING, <system-name>, Zone size of <Effective Zone Size> has over the supporting limit of <Support Zone Size> for the remote switch domain ID <Remote Switch Domain ID>.`

Probable Cause Indicates the effective zone size has exceeded the limit that a remote switch can support. The oversized portion will be truncated.

Recommended Action Reduce the zone size to 1024 or smaller, or upgrade the software of the remote switch to support 2048 zones.

Severity WARNING

NS-1006

Message `<timestamp>, [NS-1006], <sequence-number>,, WARNING, <system-name>, Duplicated WWN was detected with PID <existing device PID> and <new device PID>.`

Probable Cause Indicates that an existing device has the same WWN as a new device that has come online.

Recommended Action The switch will process the new PID and leave the existing PID intact. Subsequent switch operations will clean up the obsolete PID. However, administrators could check and remove devices with a duplicated WWN.

Severity WARNING

NS-1007

Message `<timestamp>, [NS-1007], <sequence-number>,, WARNING, <system-name>, NS has detected a logical ISL port <LISL port number> in TI zone <TI zone name> in fabric <Fabric ID>. Routing may not be setup correctly.`

Probable Cause Indicates that a logical ISL is detected in the TI zone.

Recommended Action Remove the LISL port from the TI zone because the routing may not be set up correctly.

Severity WARNING

NS-1008

Message `<timestamp>, [NS-1008], <sequence-number>,, WARNING, <system-name>, Open FR license not installed.`

Probable Cause Indicates that local devices involved in Open FR will not function without the required licensing.

Recommended Action Either install the Open FR license or relocate Open FR devices to a licensed switch.

Severity WARNING

NS-1009

Message `<timestamp>, [NS-1009], <sequence-number>,, WARNING, <system-name>, NS has detected a device with node wwn as zero, pid 0x<device PID>.`

Probable Cause Indicates that a port has logged in with node wwn as zero, DCFM wont show port connectivity.

Recommended Action Check the device that logged in. The device could be misbehaving.

Severity WARNING

NS-1010

Message `<timestamp>, [NS-1010], <sequence-number>,, WARNING, <system-name>, CSCTL mode enabled on port <csctlport> QoS zoning will be ignored for devices on this port.`

Probable Cause Indicates the CSCTL mode enabled for a port with devices as members of a QoS zone.

Recommended Action Remove CSCTL configured devices from QoS zone.

Severity WARNING

NS-1011

Message `<timestamp>, [NS-1011], <sequence-number>,, WARNING, <system-name>, NS has detected a failover flag disabled TI zone in a base switch <domain id> in fabric id <fabric id>.`

Probable Cause Indicates that a failover flag has disabled TI zone in a base switch fabric.

Recommended Action Modify failover flag to enable or remove TI zone with failover flag disabled since the routing may not be setup correctly.

Severity WARNING

Chapter

NSM System Messages

73

NSM-1001

Message `<timestamp>, [NSM-1001], <sequence-number>,, INFO, <system-name>, Interface <Interface Name> is online.`

Probable Cause Indicates that the interface is online after the protocol dependencies are resolved.

Recommended Action No action is required.

Severity INFO

NSM-1002

Message `<timestamp>, [NSM-1002], <sequence-number>,, INFO, <system-name>, Interface <Interface Name> is protocol down.`

Probable Cause Indicates that the interface is offline as one of the protocol dependencies is unresolved.

Recommended Action Check for the reason codes using the **show interface** command and resolve the protocol dependencies.

Severity INFO

NSM-1003

Message `<timestamp>, [NSM-1003], <sequence-number>,, INFO, <system-name>, Interface <Interface Name> is link down.`

Probable Cause Indicates that the interface is offline as the link is down.

Recommended Action Check whether the connectivity is proper and the remote link is up.

Severity INFO

NSM-1004

Message `<timestamp>, [NSM-1004], <sequence-number>,, INFO, <system-name>, Creating a Port-Channel interface <interface name>.`

Probable Cause Indicates that the new Portchannel interface has been created.

Recommended Action No action is required.

Severity INFO

NSM-1005

Message `<timestamp>, [NSM-1005], <sequence-number>,, INFO, <system-name>,The FCoE VLAN: <Vlan name> is in use. First remove all the FCoE sessions of its member ports and then try again to disable it.`

Probable Cause Indicates that the FCoE VLAN is used in FCoEd.

Recommended Action Disable FCoE VLAN by removing all the FCoE sessions from its member ports.

Severity INFO

NSM-1006

Message `<timestamp>, [NSM-1006], <sequence-number>,, INFO, <system-name>, FCoE on VLAN: <Vlan name> has been disabled successfully.`

Probable Cause Indicates that the FCoE is disabled on the VLAN.

Recommended Action No action is required.

Severity INFO

NSM-1007

Message `<timestamp>, [NSM-1007], <sequence-number>,, INFO, <system-name>, Chassis is <status>.`

Probable Cause Indicates the chassis is disabled or enabled.

Recommended Action No action is required.

Severity INFO

NSM-1008

Message `<timestamp>, [NSM-1008], <sequence-number>,, INFO, <system-name>, Blade <status>.`

Probable Cause Indicates the blade is disabled or enabled.

Recommended Action No action is required.

Severity INFO

NSM-1009

Message `<timestamp>, [NSM-1009], <sequence-number>,, INFO, <system-name>, Interface <InterfaceName> is deleted.`

Probable Cause Indicates that the logical interface has been deleted.

Recommended Action No action is required.

Severity INFO

NSM-1010

Message `<timestamp>, [NSM-1010], <sequence-number>,, INFO, <system-name>, InterfaceMode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.`

Probable Cause Indicates that the interface mode has been changed.

Recommended Action No action is required.

Severity INFO

NSM-1011

Message `<timestamp>, [NSM-1011], <sequence-number>,, INFO, <system-name>, OperationalEndpointMode changed from <Mode_old> to <Mode_new> for interface <InterfaceName>.`

Probable Cause Indicates that the interface OperationalEndpoint mode has been changed.

Recommended Action No action is required.

Severity INFO

NSM-1012

Message `<timestamp>, [NSM-1012], <sequence-number>,, INFO, <system-name>, Vlan classifier group <group_id> is created.`

Probable Cause Indicates that Vlan classifier group has been created.

Recommended Action No action is required.

Severity INFO

NSM-1013

Message `<timestamp>, [NSM-1013], <sequence-number>,, INFO, <system-name>, Vlan classifier group <group_id> is deleted.`

Probable Cause Indicates that Vlan classifier group has been deleted.

Recommended Action No action is required.

Severity INFO

NSM-1014

Message `<timestamp>, [NSM-1014], <sequence-number>,, INFO, <system-name>, Vlan classifier rule <rule_id> is created.`

Probable Cause Indicates that Vlan classifier rule has been created.

Recommended Action No action is required.

Severity INFO

NSM-1015

Message `<timestamp>, [NSM-1015], <sequence-number>,, INFO, <system-name>, Vlan classifier rule <rule_id> is deleted.`

Probable Cause Indicates that Vlan classifier rule has been deleted.

Recommended Action No action is required.

Severity INFO

NSM-1016

Message `<timestamp>, [NSM-1016], <sequence-number>,, INFO, <system-name>, Vlan classifier rule <rule_id> is <action> on vlan classifier group <grouip_id>.`

Probable Cause Indicates that Vlan classifier group has been modified.

Recommended Action No action is required.

Severity INFO

NSM-1017

Message `<timestamp>, [NSM-1017], <sequence-number>,, INFO, <system-name>, Interface <InterfaceName> is <action> on interface <Logical_InterfaceName>.`

Probable Cause Indicates that logical interface member list has been changed.

Recommended Action No action is required.

Severity INFO

NSM-1018

Message `<timestamp>, [NSM-1018], <sequence-number>,, INFO, <system-name>, <count> vlans <except> will be allowed on interface <Logical_InterfaceName>.`

Probable Cause Indicates that vlan membership has been changed.

Recommended Action No action is required.

Severity INFO

NSM-1019

Message `<timestamp>, [NSM-1019], <sequence-number>,, INFO, <system-name>, Interface <InterfaceName> is administratively up <Adminstatus>.`

Probable Cause Indicates that interface admin status has changed to up.

Recommended Action No action is required.

Severity INFO

NSM-1020

Message `<timestamp>, [NSM-1020], <sequence-number>,, INFO, <system-name>, Interface <InterfaceName> is administratively down <Adminstatus>.`

Probable Cause Indicates that interface admin status has changed to down.

Recommended Action No action is required.

Severity INFO

NSM-1021

Message `<timestamp>, [NSM-1021], <sequence-number>,, INFO, <system-name>, DCE ports disabled due to non-availability of core blades.`

Probable Cause Indicates that the DCE ports were brought down due to non-availability of cores.

Recommended Action Enable the DCE ports after bringing up the core blades.

Severity INFO

NSM-1022

Message `<timestamp>, [NSM-1022], <sequence-number>,, WARNING, <system-name>, <Error String>.`

Probable Cause Indicates internal error information.

Recommended Action To be transmitted to engineering for problem analysis.

Severity WARNING

Chapter

ONM System Messages

74

ONMD-1000

Message `<timestamp>, [ONMD-1000], <sequence-number>,, INFO, <system-name>, LLDP is enabled.`

Probable Cause Indicates that LLDP is globally enabled.

Recommended Action No action is required.

Severity INFO

ONMD-1001

Message `<timestamp>, [ONMD-1001], <sequence-number>,, INFO, <system-name>, LLDP is disabled.`

Probable Cause Indicates that LLDP is globally disabled.

Recommended Action No action is required.

Severity INFO

ONMD-1002

Message `<timestamp>, [ONMD-1002], <sequence-number>,, INFO, <system-name>, LLDP global configuration is changed.`

Probable Cause Indicates that LLDP Global configuration has been changed.

Recommended Action No action is required.

Severity INFO

ONMD-1003

Message `<timestamp>, [ONMD-1003], <sequence-number>,, INFO, <system-name>, LLDP is enabled on interface <InterfaceName>.`

Probable Cause Indicates that LLDP is enabled on interface.

Recommended Action No action is required.

Severity INFO

ONMD-1004

Message `<timestamp>, [ONMD-1004], <sequence-number>,, INFO, <system-name>, LLDP is disabled on interface <InterfaceName>.`

Probable Cause Indicates that LLDP is disabled on interface.

Recommended Action No action is required.

Severity INFO

Chapter

PDM System Messages

75

PDM-1001

Message `<timestamp>, [PDM-1001], <sequence-number>,, WARNING, <system-name>, Failed to parse the pdm config.`

Probable Cause Indicates the parity data manager (PDM) process could not parse the configuration file. This might be caused by a missing configuration file during the installation.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1002

Message `<timestamp>, [PDM-1002], <sequence-number>,, WARNING, <system-name>, ipcInit failed.`

Probable Cause Indicates the parity data manager (PDM) process could not initialize the inter-process communication (IPC) mechanism.

Recommended Action If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1003

Message `<timestamp>, [PDM-1003], <sequence-number>,, WARNING, <system-name>, pdm [-d] -S <service> -s <instance>.`

Probable Cause Indicates a syntax error occurred when trying to launch the parity data manager (PDM) process.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1004

Message `<timestamp>, [PDM-1004], <sequence-number>,, WARNING, <system-name>, PDM memory shortage.`

Probable Cause Indicates the parity data manager (PDM) process ran out of memory.

Recommended Action Reboot or power cycle the switch.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1005

Message `<timestamp>, [PDM-1005], <sequence-number>,, WARNING, <system-name>, FSS register failed.`

Probable Cause Indicates the parity data manager (PDM) failed to register with the Fabos synchronization service (FSS).

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1006

Message `<timestamp>, [PDM-1006], <sequence-number>,, WARNING, <system-name>, Too many files in sync.conf.`

Probable Cause Indicates the configuration file *sync.conf* contains too many entries.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1007

Message `<timestamp>, [PDM-1007], <sequence-number>,, WARNING, <system-name>, File not created: <file name> errno= <errno>.`

Probable Cause Indicates the parity data manager (PDM) process failed to create the specified file.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1008

Message `<timestamp>, [PDM-1008], <sequence-number>,, WARNING, <system-name>, Failed to get the number of U_Ports.`

Probable Cause Indicates the parity data manager (PDM) system call to **getCfg** failed.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1009

Message `<timestamp>, [PDM-1009], <sequence-number>,, WARNING, <system-name>, Can't update Port Config Data.`

Probable Cause Indicates the parity data manager (PDM) system call to **setCfg** failed.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1010

Message `<timestamp>, [PDM-1010], <sequence-number>,, WARNING, <system-name>, File open failed: <file name>, errno= <errno>.`

Probable Cause Indicates the parity data manager (PDM) process could not open the specified file.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1011

Message `<timestamp>, [PDM-1011], <sequence-number>,, WARNING, <system-name>, File read failed: <file name>, Length(read=<Number of character read>, expected=<Number of characters expected>), errno=<errno returned by read>.`

Probable Cause Indicates the parity data manager (PDM) process could not read data from the specified file.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1012

Message `<timestamp>, [PDM-1012], <sequence-number>,, WARNING, <system-name>, File write failed: <file name>. Length(read=<Number of character read>, write=<Number of characters written>), errno=<errno returned by write>.`

Probable Cause Indicates the parity data manager (PDM) process could not write data to the specified file.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1013

Message `<timestamp>, [PDM-1013], <sequence-number>,, WARNING, <system-name>, File empty: <File Name>`

Probable Cause Indicates the switch configuration file */etc/fabos/fabos.[0|1].conf* is empty.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1014

Message `<timestamp>, [PDM-1014], <sequence-number>,, WARNING, <system-name>, Access sysmod failed.`

Probable Cause Indicates a system call to **sysMod** failed.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1017

Message `<timestamp>, [PDM-1017], <sequence-number>, FFDC, CRITICAL, <system-name>, System (<Error Code>): <Command>.`

Probable Cause Indicates the specified system call failed.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

PDM-1019

Message `<timestamp>, [PDM-1019], <sequence-number>,, WARNING, <system-name>, File path or trigger too long.`

Probable Cause Indicates one line of the *pdm.conf* file is too long.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1020

Message `<timestamp>, [PDM-1020], <sequence-number>,, WARNING, <system-name>, Long path name (<Path>/<File Name>), Skip.`

Probable Cause Indicates the specified file path name is too long. The maximum character limit is 49 characters.

Recommended Action Use path names not exceeding 49 characters in length for the files to be replicated.

Severity WARNING

PDM-1021

Message `<timestamp>, [PDM-1021], <sequence-number>,, WARNING, <system-name>, Failed to download area port map.`

Probable Cause Indicates a system call failed.

Recommended Action Run the **firmwareDownload** command to reinstall the firmware.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

PDM-1022

Message

```
<timestamp>, [PDM-1022], <sequence-number>,, WARNING, <system-name>, The switch
is configured only with IPv6.
```

Probable Cause Indicates that the parity data manager (PDM) cannot synchronize with its peer because the firmware does not support IPv6.

Recommended Action Configure the local switch with IPv4 addresses.

Severity WARNING

PDM-1023

Message

```
<timestamp>, [PDM-1023], <sequence-number>,, WARNING, <system-name>, Radius is
configured for IPv6.
```

Probable Cause Indicates that the parity data manager (PDM) cannot synchronize with its peer because the Radius server is configured for IPv6 addresses. IPv6 is not supported by older firmware.

Recommended Action Configure the Radius server with IPv4 addresses.

Severity WARNING

PDM-1024

Message

```
<timestamp>, [PDM-1024], <sequence-number>,, WARNING, <system-name>, DNS is
configured for IPv6.
```

Probable Cause Indicates that the parity data manager (PDM) cannot synchronize with its peer because the domain name service (DNS) is configured for IPv6. IPv6 is not supported by older firmware.

Recommended Action Configure DNS with IPv4 addresses.

Severity WARNING

Chapter

PDTR System Messages

76

PDTR-1001

Message `<timestamp>, [PDTR-1001], <sequence-number>,, INFO, <system-name>, <informational message>.`

Probable Cause Indicates information has been written to the panic dump files. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

Recommended Action Run the **pdShow** command to view the panic dump and core dump files.

Severity INFO

PDTR-1002

Message `<timestamp>, [PDTR-1002], <sequence-number>,, INFO, <system-name>, <informational message>.`

Probable Cause Indicates information has been written to the panic dump and core dump files and a trap generated. The watchdog register codes are as follows:

- 0x10000000 bit set means that the watch dog timer (WDT) forced a core reset.
- 0x20000000 bit set means that the WDT forced a chip reset.
- All other code values are reserved.

Recommended Action Run the **pdShow** command to view the panic dump and core dump files.

Severity INFO

Chapter

PLAT System Messages

77

PLAT-1000

Message `<timestamp>, [PLAT-1000], <sequence-number>, FFDC, CRITICAL, <system-name>, <Function name> <Error string>`

Probable Cause Indicates nonrecoverable PCI errors have been detected.

Recommended Action The system will be faulted and might automatically reboot.

If the system does not reboot, then try issuing the **reboot** command from a command-line prompt.

Run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

PLAT-1001

Message `<timestamp>, [PLAT-1001], <sequence-number>,, INFO, <system-name>, CP <Identifies which CP (0 or 1) is doing the reset> resetting other CP (double reset may occur).`

Probable Cause Indicates the other CP is being reset. This message is typically generated by a CP that is in the process of becoming the active CP. Note that in certain circumstances a CP may experience a double reset and reboot twice in a row. A CP can recover automatically even if it has rebooted twice.

Recommended Action No action is required.

Severity INFO

PLAT-1002

Message `<timestamp>, [PLAT-1002], <sequence-number>,, CRITICAL, <system-name>, CP <Identifies which CP (0 or 1) is generating the message>: <Error message> CP Fence <CP Fence register. Contents (2 bytes) are platform-specific> <CP Error register. Contents are platform-specific> CP Error <CP Error register. Contents are platform-specific>.`

Probable Cause Indicates that the CP cannot access the I2C subsystem either because of an error condtion or being fenced or isolated from the I2C bus.

Recommended Action Reboot the CP if it does not reboot itself. Reseat the CP if rebooting does not solve the problem. If the problem still persists, then replace the CP.

Severity CRITICAL

PLAT-1003

Message `<timestamp>, [PLAT-1003], <sequence-number>, FFDC, CRITICAL, <system-name>, <Info message> Slot <Blade Slot number> C/BE: <Captured Command/Byte-Enables data> ADBUS: <Captured AD bus data> misc_intr <Bridge reset interrupts>.`

Probable Cause Indicates a PCI bus hang was detected.

Recommended Action The FRU must be replaced.

Severity CRITICAL

Chapter

PMGR System Messages

78

PMGR-1001

Message `<timestamp>, [PMGR-1001], <sequence-number>, INFO, <system-name>, Attempt to create switch <FID> succeeded.`

Probable Cause Indicates that the switch with the specified FID was successfully created.

Recommended Action No action is required.

Severity INFO

PMGR-1002

Message `<timestamp>, [PMGR-1002], <sequence-number>, WARNING, <system-name>, Attempt to create switch <FID> failed.  Error message: <Error Message>.`

Probable Cause Indicates that the switch with the specified FID was not created.

Recommended Action No action is required.

Severity WARNING

PMGR-1003

Message `<timestamp>, [PMGR-1003], <sequence-number>, INFO, <system-name>, Attempt to delete switch <FID> succeeded.`

Probable Cause Indicates that the switch with the specified FID was successfully deleted.

Recommended Action No action is required.

Severity INFO

PMGR-1004

Message `<timestamp>, [PMGR-1004], <sequence-number>, WARNING, <system-name>,Attempt to create switch <FID> failed. Error message: <Error Message>.`

Probable Cause Indicates that the switch with the specified FID was not deleted.

Recommended Action No action is required.

Severity WARNING

PMGR-1005

Message `<timestamp>, [PMGR-1005], <sequence-number>, INFO, <system-name>, Attempt to move port(s) <Ports> on slot <Slot> to switch <FID> succeeded.`

Probable Cause Indicates the successful attempt to move the ports to the specified switch.

Recommended Action No action is required.

Severity INFO

PMGR-1006

Message `<timestamp>, [PMGR-1006], <sequence-number>, WARNING, <system-name>, Attempt to move port(s) <Ports> on slot <Slot> to switch <FID> failed.  Error message: <Error Message>.`

Probable Cause Indicates the unsuccessful attempt to move the ports to the specified switch.

Recommended Action No action is required.

Severity WARNING

PMGR-1007

Message `<timestamp>, [PMGR-1007], <sequence-number>, INFO, <system-name>, Attempt to change switch <FID> to switch <New FID> succeeded.`

Probable Cause Indicates the successful change of the switch FID.

Recommended Action No action is required.

Severity INFO

PMGR-1008

Message `<timestamp>, [PMGR-1008], <sequence-number>, WARNING, <system-name>,Attempt to change switch <FID> to switch <New FID> failed.  Error message: <Error Message>.`

Probable Cause Indicates the failed attempt to change the switch FID.

Recommended Action No action is required.

Severity WARNING

PMGR-1009

Message `<timestamp>, [PMGR-1009], <sequence-number>, INFO, <system-name>,Attempt to change the base switch to switch <FID> succeeded.`

Probable Cause Indicates the successful change of the base switch.

Recommended Action No action is required.

Severity INFO

PMGR-1010

Message `<timestamp>, [PMGR-1010], <sequence-number>, WARNING, <system-name>, Attempt to change the base switch to switch <FID> failed.  Error message: <Error Message>.`

Probable Cause Indicates the failed attempt to change the base switch.

Recommended Action No action is required.

Severity WARNING

PMGR-1011

Message `<timestamp>, [PMGR-1011], <sequence-number>, INFO, <system-name>, Attempt to move ports to switch <FID> succeeded.`

Probable Cause Indicates the successful attempt to move the ports to the specified switch.

Recommended Action No action is required.

Severity INFO

Chapter

PORT System Messages

79

PORT-1003

Message `<timestamp>, [PORT-1003], <sequence-number>,, WARNING, <system-name>, Port <port number> Faulted because of many Link Failures`

Probable Cause Indicates that the specified port is now disabled because the link on this port had multiple failures that exceeded an internally set threshold on the port. This problem is typically related to hardware.

Recommended Action Check and replace (if necessary) the hardware attached to both ends of the specified *port number*, including:

- the media (SFPs)
- the cable (fiber optic or copper ISL)
- the attached devices

When finished checking the hardware, perform the **portEnable** command to re-enable the port.

Severity WARNING

PORT-1004

Message `<timestamp>, [PORT-1004], <sequence-number>,, INFO, <system-name>, Port <port number> (<port number (hex)>) could not be enabled because it is disabled due to long distance.`

Probable Cause Indicates the specified port is not enabled because other ports in the same group have used the buffers for this port group. This happens when other ports were configured to be long distance.

Recommended Action To enable this port, reconfigure the other E_Ports so they are not long distance or change the other E_Ports so they are not E_Ports. This will free some buffers and allow this port to be enabled.

Severity INFO

PORT-1005

Message `<timestamp>, [PORT-1005], <sequence-number>,, WARNING, <system-name>, Slot <slot number> port <port on slot> does not support configured L_port. Issue portCfgLport to clear configuration.`

Probable Cause Indicates the specified port is configured to be an L_port, but the port does not support L_port. If an L_port is connected, then the port will be disabled because the port does not support L_port. If an E_port or F_port is connected, then the port will not come up since it is configured to be an L_port.

Recommended Action Invoke the **portCfgLport** command to clear the L_port configuration.

Severity WARNING

PORT-1006

Message `<timestamp>, [PORT-1006], <sequence-number>,, INFO, <system-name>, Configuration changed for port (ID: <port number>) in No_Module or No_Light state.`

Probable Cause Indicates the configuration changes were made to an offline port in No_Module or No_Light state.

Recommended Action No action is required.

Severity INFO

PORT-1007

Message `<timestamp>, [PORT-1007], <sequence-number>,, INFO, <system-name>, Port (ID: <potr number>) has been renamed to <port name>.`

Probable Cause Indicates a port has been reconfigured with a different name.

Recommended Action No action is required.

Severity INFO

PORT-1008

Message `<timestamp>, [PORT-1008], <sequence-number>,, INFO, <system-name>, GigE Port (ID: <port number>) has been enabled.`

Probable Cause Indicates a GbE port has been enabled.

Recommended Action No action is required.

Severity INFO

PORT-1009

Message `<timestamp>, [PORT-1009], <sequence-number>,, INFO, <system-name>, GigE Port (ID: <port number>) has been disabled.`

Probable Cause Indicates a GbE port has been disabled.

Recommended Action No action is required.

Severity INFO

PORT-1010

Message `<timestamp>, [PORT-1010], <sequence-number>,, WARNING, <system-name>, Port (ID: <port number>) QOS is disabled.`

Probable Cause The Port QOS is disabled because the port currently has Best Effort Setting that requires QOS to be disabled on a 4G or 8G long distance platform.

Recommended Action This is normal; no action required.

Severity WARNING

Chapter

PS System Messages

80

PS-1000

Message `<timestamp>, [PS-1000], <sequence-number>, FFDC, CRITICAL, <system-name>, Failed to initialize Advanced Performance Monitoring.`

Probable Cause Indicates an unexpected software error has occurred in Advanced Performance Monitoring (APM). The performance monitor has failed to initialize.

Recommended Action The control processor (CP) should restart (or fail over) automatically If this does not happen, restart or power cycle the switch to re-initiate the firmware.

Severity CRITICAL

PS-1001

Message `<timestamp>, [PS-1001], <sequence-number>,, INFO, <system-name>, Advanced Performance Monitoring configuration updated due to change in PID format`

Probable Cause Indicates the PID format was changed.

Recommended Action No action is required. Refer to the *Fabric OS Administrator's Guide* for more information on the PID format.

Severity INFO

PS-1002

Message `<timestamp>, [PS-1002], <sequence-number>,, INFO, <system-name>, Failed to initialize the tracing system for Advanced Performance Monitoring.`

Probable Cause Indicates an unexpected software error has occurred in Advanced Performance Monitoring (APM). The performance monitor tracing system has failed to initialize.

Recommended Action Tracing will not be available for Advanced Performance Monitoring (APM), but other functions will be normal. To activate tracing, restart (or fail over) the control processor (CP).

Severity INFO

PS-1003

Message `<timestamp>, [PS-1003], <sequence-number>,, WARNING, <system-name>, Failed to set end-to-end monitoring mask on ISL ports.`

Probable Cause Indicates that the restoring configuration has failed to set the end-to-end monitoring mask on at least one ISL port.

Recommended Action No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

Severity WARNING

PS-1004

Message `<timestamp>, [PS-1004], <sequence-number>,, WARNING, <system-name>, Failed to add end-to-end monitors on port <port> which is an ISL port.`

Probable Cause Indicates that the restoring configuration has attempted to add end-to-end monitors on at least one ISL port.

Recommended Action No action is required. End-to-end monitoring is not supported on ISL ports when ISL monitoring is enabled. ISL monitoring can only be disabled through the Fabric Access API.

Severity WARNING

PS-1005

Message `<timestamp>, [PS-1005], <sequence-number>,, WARNING, <system-name>, ISL monitor on port <port> stopped counting because no hardware resources are available`

Probable Cause Indicates that ISL and end-to-end monitors have used up all hardware resources.

Recommended Action To resume counting, delete some end-to-end monitors sharing the same hardware resource pool.

Severity WARNING

PS-1006

Message `<timestamp>, [PS-1006], <sequence-number>,, WARNING, <system-name>, Failed to add fabricmode toptalker monitors on domain=<domain id>, because end-to-end monitors are configured on this switch.`

Probable Cause Indicates the end-to-end monitors are configured on the switch.

Recommended Action Delete the end-to-end monitors on that switch and re-install the fabricmode TopTalker monitor. End-to-end monitors and fabricmode Top Talker monitors are mutually exclusive.

Severity WARNING

PS-1007

Message `<timestamp>, [PS-1007], <sequence-number>,, WARNING, <system-name>, Failed to add fabricmode toptalker on domain=<domain id>. <function name>.`

Probable Cause Indicates that FCR or McData mode is enabled on this particular fabric.

Recommended Action No action required. Top Talker cannot be installed on fabric with FC router or McData mode enabled. In case if the top talker has to be installed on fabric, FC router and McData mode has to be disabled.

Severity WARNING

Chapter

PSWP System Messages

81

PSWP-1001

Message `<timestamp>, [PSWP-1001], <sequence-number>,, INFO, <system-name>, PID for port <wwn name corresponding to source port> and port <wwn name corresponding to destination port> are swapped. New PID for port <wwn name corresponding to source port> is <wwn name corresponding to destination port> and port <new area corresponding to source wwn> is <new area corresponding to destination wwn>.`

Probable Cause Indicates that the **portSwap** command has been issued.

Recommended Action No action is required.

Severity INFO

PSWP-1002

Message `<timestamp>, [PSWP-1002], <sequence-number>,, INFO, <system-name>, Port Swap feature enabled.`

Probable Cause Indicates that the **portSwap** feature has been enabled in the switch.

Recommended Action No action is required.

Severity INFO

PSWP-1003

Message `<timestamp>, [PSWP-1003], <sequence-number>,, INFO, <system-name>, Port Swap feature disabled.`

Probable Cause Indicates that the **portSwap** command feature has been disabled in the switch.

Recommended Action No action is required.

Severity INFO

PSWP-1004

Message `<timestamp>, [PSWP-1004], <sequence-number>,, INFO, <system-name>, Blade Swap complete for slots <slot number corresponding to the source blade> and <slot number corresponding to the destination blade>.`

Probable Cause Indicates that the **bladeSwap** command has been issued.

Recommended Action No action is required.

Severity INFO

PSWP-1005

Message `<timestamp>, [PSWP-1005, <sequence-number>,, WARNING, <system-name>, Blade Swap undo failed with error code <error code from undoBladeSwap>.`

Probable Cause Indicates that the **bladeSwap** undo command has failed.

Recommended Action Use the **portSwapShow** command to display a list of currently swapped ports. Then use the **portSwap** command to acheive the desired result.

Severity WARNING

PSWP-1006

Message `<timestamp>, [PSWP-1006, <sequence-number>,, WARNING, <system-name>, Blade Swap failed on configInit with error code <error code from configInit.>in switch number <current switch number>.`

Probable Cause Indicates that the **bladeSwap** command has failed to access the configuration data.

Recommended Action Retry the command. If the failure persists, contact your support representative.

Severity WARNING

PSWP-1007

Message `<timestamp>, [PSWP-1007, <sequence-number>,, WARNING, <system-name>, Blade Swap failed on fabosInit with error code <error code from fabosInit.>in switch number <current switch number>.`

Probable Cause Indicates that the **bladeSwap** command has failed to access the switch context.

Recommended Action Retry the command. If the failure persists, contact your support representative.

Severity WARNING

Chapter

RAS System Messages

82

RAS-1001

Message `<timestamp>, [RAS-1001], <sequence-number>,, INFO, <system-name>, First failure data capture (FFDC) event occurred.`

Probable Cause Indicates that a failure data event was captured.

Recommended Action Run the **supportFtp** command (as needed) to set up automatic FTP transfers and run the **supportSave** command then contact your switch service provider.

Severity INFO

RAS-1002

Message `<timestamp>, [RAS-1002], <sequence-number>,, WARNING, <system-name>, First failure data capture (FFDC) maximum storage size (<log size limit> MB) was reached.`

Probable Cause Indicates that the maximum storage size for FFDC data capture is reached.

Recommended Action Run the **supportSave** command and contact your switch service provider.

Severity WARNING

RAS-1004

Message `<timestamp>, [RAS-1004], <sequence-number>, FFDC, WARNING, <system-name>, Software 'verify' error detected.`

Probable Cause Indicates an internal software error.

Recommended Action Run the **supportSave** command and contact your switch service provider.

Severity WARNING

RAS-1005

Message `<timestamp>, [RAS-1005], <sequence-number>, FFDC, WARNING, <system-name>, Software 'assert' error detected.`

Probable Cause Indicates an internal software error.

Recommended Action Run the **supportSave** command and contact your switch service provider.

Severity WARNING

RAS-1006

Message `<timestamp>, [RAS-1006], <sequence-number>, INFO, <system-name>, Support data file (<Uploaded file name>) automatically transferred to remote address ' <Remote target designated by user> '.`

Probable Cause Indicates that the support data file is transferred from the switch automatically.

Recommended Action No action is required.

Severity INFO

RAS-2001

Message `<timestamp>, [RAS-2001], <sequence-number>, INFO, <system-name>, Audit message log is enabled.`

Probable Cause Indicates that the audit message log is enabled.

Recommended Action No action is required.

Severity INFO

RAS-2002

Message `<timestamp>, [RAS-2002], <sequence-number>, INFO, <system-name>, Audit message log is disabled.`

Probable Cause Indicates that the audit message log is disabled.

Recommended Action No action is required.

Severity INFO

RAS-2003

Message `<timestamp>, [RAS-2003], <sequence-number>, INFO, <system-name>, Audit message class configuration has been changed to <New audit class configuration>.`

Probable Cause Indicates that the configured classes of the audit feature have been changed.

Recommended Action No action is required.

Severity INFO

RAS-3001

Message `<timestamp>, [RAS-3001], <sequence-number>, INFO, <system-name>, USB storage device plug-in detected.`

Probable Cause Indicates that the USB storage device plug-in is being detected.

Recommended Action No action is required.

Severity INFO

RAS-3002

Message `<timestamp>, [RAS-3002], <sequence-number>, INFO, <system-name>, USB storage device enabled.`

Probable Cause Indicates that the USB storage device is enabled.

Recommended Action No action is required.

Severity INFO

RAS-3003

Message `<timestamp>, [RAS-3003], <sequence-number>, WARNING, <system-name>, USB storage device was unplugged before it was disabled.`

Probable Cause Indicates that the USB storage device was unplugged before it was disabled.

Recommended Action No action is required.

Severity WARNING

RAS-3004

Message `<timestamp>, [RAS-3004], <sequence-number>, INFO, <system-name>, USB storage device disabled.`

Probable Cause Indicates that the USB storage device is disabled.

Recommended Action No action is required.

Severity INFO

Chapter

RCS System Messages

83

RCS-1001

Message `<timestamp>, [RCS-1001], <sequence-number>,, INFO, <system-name>, RCS has been disabled. Some switches in the fabric do not support this feature.`

Probable Cause Indicates that the RCS feature has been disabled on the local switch because not all switches in the fabric support RCS or the switch is in nonnative mode.

Recommended Action Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and later, and v4.1 and later.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

Severity INFO

RCS-1002

Message `<timestamp>, [RCS-1002], <sequence-number>,, INFO, <system-name>, RCS has been enabled.`

Probable Cause Indicates that the RCS feature has been enabled. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

Recommended Action No action is required.

Severity INFO

RCS-1003

Message `<timestamp>, [RCS-1003], <sequence-number>,, ERROR, <system-name>, Failed to allocate memory: (<function name>)`

Probable Cause Indicates that the specified RCS function failed to allocate memory.

Recommended Action This message is usually transitory. Wait for a few minutes and retry the command.

Check the memory usage on the switch using the **memShow** command.

Restart or power cycle the switch.

Severity ERROR

RCS-1004

Message `<timestamp>, [RCS-1004], <sequence-number>,, ERROR, <system-name>, Application(<application name>) not registered.(<error string>)`

Probable Cause Indicates that a specified application did not register with RCS.

Recommended Action Run the **haShow** command to view the HA state.

Run the **haDisable** and the **haEnable** commands.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS is supported in Fabric OS v2.6, v3.1 and later, and v4.1 and later.

Run the **firmwareDownload** command to upgrade the firmware for any switches that do not support RCS.

Severity ERROR

RCS-1005

Message `<timestamp>, [RCS-1005], <sequence-number>,, INFO, <system-name>, Phase <RCS phase>, <Application Name> Application returned <Reject reason>, 0x<Reject code>.`

Probable Cause Indicates that a receiving switch is rejecting an RCS phase.

Recommended Action If the reject is in ACA phase, wait for a few minutes and then retry the operation from the sender switch.

If the reject is in the SFC phase, check if the application license exists for the local domain and if the application data is compatible.

Severity INFO

RCS-1006

Message `<timestamp>, [RCS-1006], <sequence-number>,, INFO, <system-name>, State <RCS phase>, Application <Application Name> AD<Administrative Domain>, RCS CM. Domain <Domain ID that sent the reject> returned 0x<Reject code>. App Response Code <Application Response Code>`

Probable Cause Indicates that a remote domain rejected an RCS phase initiated by an application on the local switch.

If the reject phase is ACA, the remote domain might be busy and could not process the new request.

If the reject phase is SFC, the data sent by the application might not be compatible or the domain does not have the license to support that application.

Recommended Action If the reject is in ACA phase, wait for a few minutes and then retry the operation.

If the reject is in the SFC phase, check if the application license exists for the remote domain and if the application data is compatible.

Severity INFO

RCS-1007

Message `<timestamp>, [RCS-1007], <sequence-number>,, ERROR, <system-name>, Zone DB size and propogation overhead exceeds domain <domain number>'s maximum supported Zone DB size <max zone db size>. Retry after reducing the Zone DB size.`

Probable Cause Indicates that a domain cannot handle the zone database being committed.

Recommended Action Reduce the zone database size.

Severity ERROR

RCS-1008

Message `<timestamp>, [RCS-1008], <sequence-number>,, ERROR, <system-name>, Domain <domain number> Lowest Max Zone DB size`

Probable Cause Indicates that the domain has the lowest maximum zone database size.

Recommended Action Reduce the zone database size.

Severity ERROR

Chapter

RKD System Messages

84

RKD-1001

Message `<timestamp>, [RKD-1001], <sequence-number>,, INFO, <system-name>, <Re-key type (First time encryption/Rekey/Write Metadata)> operation <Re-key action (started/completed/cancelled)>.\nTarget: <Target physial WWN>, Initiator: <Initiator physical WWN>, LUN ID: <LUN ID>.\n SessionId:<Session ID>/<Session MN>`

Probable Cause Indicates that a First time encryption/re-key/Write Metadata was started/completed/cancelled.

Recommended Action No action is required.

Severity INFO

RKD-1002

Message `<timestamp>, [RKD-1002], <sequence-number>,, ERROR, <system-name>, Could not start <Re-key type (First time encryption/Rekey/Write Metadata)> operation.\n<I/T/L String>.\n No response from cluster member WWN: <EE WWN> Slot: <EE Slot Number>.`

Probable Cause Indicates that a First time encryption/re-key/Write Metadata was not started.

Recommended Action Correct the Cluster Ethernet link error and retry.

Severity ERROR

RKD-1003

Message `<timestamp>, [RKD-1003], <sequence-number>,, CRITICAL, <system-name>, <Re-key type (First time encryption/Rekey/Write Metadata)> encountered a FATAL SCSI error and will be suspended.\n<I/T/L String>.\nCommand: <Read/Write>\nLBA: <LBA>\nNum Blocks: <Num of Blocks>\nError: <Error String>\nSK/ASC: <SCSI Sense Key>/<SCSI ASC>.`

Probable Cause Indicates that a First time encryption/re-key/Write Metadata encountered a fatal SCSI error and was suspended.

Recommended Action Correct the error and resume.

Severity CRITICAL

RKD-1004

Message `<timestamp>, [RKD-1004], <sequence-number>,, INFO, <system-name>, Message: <Generic rekey message>.`

Probable Cause Indicates the generic rekey message.

Recommended Action No action is required.

Severity INFO

RKD-1005

Message `<timestamp>, [RKD-1005], <sequence-number>,, WARNING, <system-name>, LUN with LSN: <LUN LSN> does no have metadata. Please make note of key ID <Key ID for encrypt/decrypt> that will be used for encryption/decryption of the LUN.`

Probable Cause Indicates an uncompressible data on blocks 1-16 of the LUN.

Recommended Action Migrate the data on this LUN to a larger LUN and add it to the container with -newLUN option.

Severity WARNING

Chapter

RMOND System Messages

85

RMON-1001

Message `<timestamp>, [RMON-1001], <sequence-number>,, INFO, <system-name>, RMON rising threshold alarm from SNMP OID <oid>.`

Probable Cause Indicates that the threshold level has exceeded for the sample type of RMON alarm.

Recommended Action Check the traffic on the interface.

Severity INFO

RMON-1002

Message `<timestamp>, [RMON-1002], <sequence-number>,, INFO, <system-name>, RMON falling threshold alarm from SNMP OID <oid>.`

Probable Cause Indicates that the threshold level has reduced for the sample type of RMON alarm.

Recommended Action Check the traffic on the interface.

Severity INFO

Chapter

RPCD System Messages

86

RPCD-1001

Message `<timestamp>, [RPCD-1001], <sequence-number>,, WARNING, <system-name>, Authentication Error: client \"<IP address>\" has bad credentials: <bad user name and password pair>`

Probable Cause Indicates an authentication error was reported. The specified *client IP address* has faulty credentials.

Recommended Action Enter the correct user name and password from the Fabric Access API host.

Severity WARNING

RPCD-1002

Message `<timestamp>, [RPCD-1002], <sequence-number>,, WARNING, <system-name>, Missing certificate file. Secure RPCd is disabled.`

Probable Cause Indicates an SSL certificate is missing.

Recommended Action To enable RPCD in secure mode, install a valid SSL certificate on the switch.

Severity WARNING

RPCD-1003

Message `<timestamp>, [RPCD-1003], <sequence-number>,, WARNING, <system-name>, Permission denied accessing certificate file. Secure RPCd is disabled.`

Probable Cause Indicates the SSL certificate file configured on the switch could not be accessed because the root did not have read-level access.

Recommended Action Change the file system access level for the certificate to root read-level access.

Severity WARNING

RPCD-1004

Message `<timestamp>, [RPCD-1004], <sequence-number>,, WARNING, <system-name>, Invalid certificate file. Secure RPCd is disabled.`

Probable Cause Indicates the SSL certificate file has been corrupted.

Recommended Action To enable RPCD in Secure mode, install a valid SSL certificate in the switch.

Severity WARNING

RPCD-1005

Message `<timestamp>, [RPCD-1005], <sequence-number>,, WARNING, <system-name>, Missing private key file. Secure RPCd is disabled.`

Probable Cause Indicates the private key file is missing.

Recommended Action Run the **pkiCreate** command to install a valid private key file.

Severity WARNING

RPCD-1006

Message `<timestamp>, [RPCD-1006], <sequence-number>,, WARNING, <system-name>, Permission denied accessing private key file. Secure RPCd is disabled.`

Probable Cause Indicates the private key file configured on the switch could not be accessed because the root did not have read-level access.

Recommended Action Change the file system access level for the private key file and make sure that the root has read-level access.

Severity WARNING

RPCD-1007

Message `<timestamp>, [RPCD-1007], <sequence-number>,, WARNING, <system-name>, Invalid private file. Secure RPCd is disabled.`

Probable Cause Indicates the private key file has been corrupted.

Recommended Action Run the **pkiCreate** command to install a valid private key file.

Severity WARNING

Chapter

RTWR System Messages

87

RTWR-1001

Message `<timestamp>, [RTWR-1001], <sequence-number>,, ERROR, <system-name>, RTWR <routine: error message> 0x<detail 1>, 0x<detail 2>, 0x<detail 3>, 0x<detail 4>, 0x<detail 5>`

Probable Cause Indicates that an error has occurred in the RTWR. The message provides the name of the routine having the error, and more specific error information. The values from 1 through 5 provide more information.

Recommended Action No action is required.

Severity ERROR

RTWR-1002

Message `<timestamp>, [RTWR-1002], <sequence-number>,, WARNING, <system-name>, RTWR <error message> 0x<detail1>, 0x<detail2>, 0x<detail3>, 0x<detail4>, 0x<detail5>`

Probable Cause Indicates that the RTWR has exhausted the maximum number of retries by sending data to the specified domain. Possible detail values include:

- RTWRTransmit: Max retries exhausted
- detail1: Port
- detail2: Domain
- detail3: Retry Count
- detail4: Status
- detail5: Process ID

Recommended Action Run the **fabricShow** command to see if the specified domain ID is online.

Enable the switch with the specified domain ID.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers and run the **supportSave** command then contact your switch service provider.

Severity WARNING

RTWR-1003

Message `<timestamp>, [RTWR-1003], <sequence-number>,, INFO, <system-name>, <module name>: RTWR retry <number of times retried> to domain <domain ID>, iu_data <first word of iu_data>`

Probable Cause Indicates the number of times the RTWR has failed to get a response.

Recommended Action Run the **dom** command to verify that the specified domain ID is reachable.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers and run the **supportSave** command then contact your switch service provider.

Severity INFO

Chapter

SAS System Messages

88

SAS-1001

Message `<timestamp>, [SAS-1001], <sequence-number>,, ERROR, <system-name>, string description of command which failed> of GE <GE port number which failed> failed. Please retry the command. Data inst=<chip instance> st=<chip init state> rsn=<failure reason> fn=<message function> oid=<chip OID>.`

Probable Cause The Hardware is not responding to the command request; possibly because it is busy.

Recommended Action Retry the command.

Severity ERROR

Chapter

SCN System Messages

89

SCN-1001

Message

```
<timestamp>, [SCN-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, SCN
queue overflow for process <daemon name>
```

Probable Cause

Indicates that an attempt to write a state change notification (SCN) message to a specific queue has failed because the SCN queue for the specified *daemon name* is full. This might be caused by the daemon hanging or the system being busy.

Some valid values for *daemon name* are listed below. For a complete listing, see the Introduction to this manual.

- fabricd
- asd
- evmd
- fcpd
- webd
- msd
- nsd
- psd
- snmpd
- zoned
- fspfd
- tsd

Recommended Action

If this message is caused by the system being busy, the condition is temporary.

If this message is caused by a hung daemon, the software watchdog will cause the daemon to dump the core and reboot the switch. In this case, run the **supportSave** command to send the core files using FTP to a secure server location.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

CRITICAL

Chapter

SEC System Messages

90

SEC-1001

Message

```
<timestamp>, [SEC-1001], <sequence-number>,, ERROR, <system-name>, RCS process
fails: <reason code>
```

Probable Cause

Indicates that the reliable commit service (RCS) process failed to complete. RCS is a mechanism for transferring data from one switch to other switches within the fabric. RCS ensures that either all or none of the switches commit to the database. RCS can fail if one switch in the fabric is busy or in an error state that prevents it from accepting the database.

Recommended Action

The RCS process is invoked when the security database is modified by a security command (for example, the **secPolicySave** command, the **secPolicyActivate** command, or the **secVersionReset** command). If the switch is busy, the command might fail the first time. Retry the command.

Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, RCS is automatically enabled.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity

ERROR

SEC-1002

Message

```
<timestamp>, [SEC-1002], <sequence-number>,, ERROR, <system-name>, Security data
fails: <Reason Text>.
```

Probable Cause

Indicates that the receiving switch fails to validate the security database sent from the primary fabric configuration server (FCS) switch. This might be caused by several factors: the data package may be corrupted, the time stamp on the package may be out of range as a result of replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure may result from an internal error, such as losing the primary public key or an invalid database.

Recommended Action

Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in *Ready* state. If a switch is in the error state, the database might not be correctly updated for that switch. The error might also be a result of an internal corruption or a hacker attack to the secure fabric. If you have a reason to believe that the error is the result of a possible security breach, take appropriate action as defined by your enterprise security policy.

Severity

ERROR

SEC-1003

Message `<timestamp>, [SEC-1003], <sequence-number>,, WARNING, <system-name>, Fail to download security data to domain <Domain number> after <Number of retires> retries`

Probable Cause Indicates the specified domain has failed to download security data after the specified number of attempts, and that the failed switch encountered an error accepting the database download. The primary switch will segment the failed switch after 30 tries.

Recommended Action Reset the version stamp on the switch to '0' using the **secVersionReset** command and then rejoin the switch to the fabric.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

SEC-1005

Message `<timestamp>, [SEC-1005], <sequence-number>,, INFO, <system-name>, Primary FCS receives data request from domain <Domain number>`

Probable Cause Indicates the primary fabric configuration server (FCS) received a data request from the specified domain. For example, if the switch fails to update the database or is attacked (data injection), a message is generated to the primary FCS to try to correct and resync with the rest of the switches in the fabric.

Recommended Action Use the **secFabricShow** command to check whether any of the switches in the fabric encountered an error. If one or more switches is not in the Ready state, and you have reason to believe that the error is the result of a possible security breach, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1006

Message `<timestamp>, [SEC-1006], <sequence-number>,, WARNING, <system-name>, Security statistics error: Failed to reset due to invalid <data>.`

Probable Cause Indicates that invalid data has been received for any statistic-related command for security (**secStatsShow** or **secStatsReset**). The counter is updated automatically when a security violation occurs. This message might also occur if the updating counter fails.

Recommended Action If the message is the result of a user command, retry the statistic command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

SEC-1007

Message `<timestamp>, [SEC-1007], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish API connection.`

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the API connection.

Severity INFO

SEC-1008

Message `<timestamp>, [SEC-1008], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish HTTP connection.`

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the HTTP connection.

Severity INFO

SEC-1009

Message `<timestamp>, [SEC-1009], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish TELNET connection.`

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the Telnet connection.

Severity INFO

SEC-1010

Message `<timestamp>, [SEC-1010], <sequence-number>,, ERROR, <system-name>, RCS rejected <Reason String>.`

Probable Cause Trying to distribute the database from a non primary switch. Resolved the above specified error.

Recommended Action Resolve the above specifed error by executing the command only from Primary FCS.

Severity ERROR

SEC-1016

Message `<timestamp>, [SEC-1016], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized host with IP address <IP address of the violating host> tries to establish SSH connection.`

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the SSH connection.

Severity INFO

SEC-1022

Message `<timestamp>, [SEC-1022], <sequence-number>,, WARNING, <system-name>, Failed to <operation> PKI objects.`

Probable Cause Indicates the fabric has failed to generate or validate either the public or private key pair or the certificate signing request (CSR).

Recommended Action Run the **pkiShow** command and verify that all public key infrastructure (PKI) objects exist on the switch. If the private key does not exist, follow the steps for re-creating PKI objects, outlined in the *Secure Fabric OS Administrator's Guide.* If a certificate does not exist or is invalid, install the certificate by following the field upgrade process.

Severity WARNING

SEC-1024

Message `<timestamp>, [SEC-1024], <sequence-number>,, INFO, <system-name>, The <DB name> security database is too large to fit in flash.`

Probable Cause Indicates the size of the security database is too large for the flash memory. The size of the security database increases with the number of entries in each policy.

Recommended Action Reduce the size of the security database by reducing the number of entries within each policy.

Severity INFO

SEC-1025

Message `<timestamp>, [SEC-1025], <sequence-number>,, ERROR, <system-name>, Invalid IP address (<IP address>) detected.`

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1026

Message `<timestamp>, [SEC-1026], <sequence-number>,, ERROR, <system-name>, Invalid format or character in switch member <switch member ID>.`

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1028

Message `<timestamp>, [SEC-1028], <sequence-number>,, ERROR, <system-name>, No name is specified.`

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1029

Message `<timestamp>, [SEC-1029], <sequence-number>,, ERROR, <system-name>, Invalid character in <policy name>.`

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1030

Message `<timestamp>, [SEC-1030], <sequence-number>, ERROR, <system-name>, The length of the name invalid.`

Probable Cause Indicates a corruption occurred during the distribution of the security database. This can occur only when the primary fabric configuration server (FCS) distributes the security database to the other switches in the fabric, then local validation finds the error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1031

Message `<timestamp>, [SEC-1031], <sequence-number>,, WARNING, <system-name>, Current security policy DB cannot be supported by standby. CPs will go out of sync.`

Probable Cause Indicates the security database size is not supported by the standby control processor (CP).

Recommended Action Reduce the security policy size by deleting entries within a policy or by deleting some policies.

Severity WARNING

SEC-1032

Message `<timestamp>, [SEC-1032], <sequence-number>,, ERROR, <system-name>, Empty FCS list is not allowed.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1033

Message `<timestamp>, [SEC-1033], <sequence-number>,, ERROR, <system-name>, Invalid character used in member parameter to add switch to SCC policy; command terminated.`

Probable Cause Indicates a member parameter in the **secPolicyAdd** command is invalid (e. g., it may include an invalid character, such as an asterisk). A valid switch identifier (a WWN, a domain ID, or a switch name) must be provided as a member parameter in the **secPolicyAdd** command. Only the **secPolicyCreate** command supports use of the asterisk for adding switches to policies.

Recommended Action Run the **secPolicyAdd** command using a valid switch identifier (WWN, domain ID, or switch name) to add specific switches to the switch connection control (SCC) policy.

Refer to the *Fabric OS Command Reference* for more information on the **secPolicyAdd** and **secPolicyCreate** commands.

Severity ERROR

SEC-1034

Message `<timestamp>, [SEC-1034], <sequence-number>,, ERROR, <system-name>, Invalid member <policy member>.`

Probable Cause Indicates the input list has an invalid member.

Recommended Action Verify the member names, and input the correct information.

Severity ERROR

SEC-1035

Message `<timestamp>, [SEC-1035], <sequence-number>,, ERROR, <system-name>, Invalid device WWN <device WWN>.`

Probable Cause Indicates the specified world wide name (WWN) is invalid.

Recommended Action Enter the correct WWN value.

Severity ERROR

SEC-1036

Message `<timestamp>, [SEC-1036], <sequence-number>,, ERROR, <system-name>, Device name <device name> is invalid due to a missing colon.`

Probable Cause Indicates one or more device names mentioned in the **securePolicyCreate** or **securePolicyAdd** command does not have the colon character (:) as required.

Recommended Action Run the **secPolicyCreate** or **secPolicyAdd** command with a properly formatted device name parameter.

Severity ERROR

SEC-1037

Message `<timestamp>, [SEC-1037], <sequence-number>,, ERROR, <system-name>, Invalid WWN format <invalid WWN>.`

Probable Cause Indicates the world wide name (WWN) entered in the policy member list had an invalid format.

Recommended Action Run the command again using the standard WWN format, 16 hexadecimal digits grouped as eight colon separated pairs. For example: 50:06:04:81:D6:F3:45:42.

Severity ERROR

SEC-1038

Message `<timestamp>, [SEC-1038], <sequence-number>,, ERROR, <system-name>, Invalid domain <domain ID>.`

Probable Cause Indicates an invalid domain ID was entered.

Recommended Action Verify that the domain ID is correct. If it is not, then re-run the command using the correct domain ID.

Severity ERROR

SEC-1040

Message `<timestamp>, [SEC-1040], <sequence-number>,, ERROR, <system-name>, Invalid portlist (<port list>). Cannot combine * with port member in the same portlist.`

Probable Cause Indicates the port list contains the wildcard asterisk (*) character. You cannot use the asterisk in a port list.

Recommended Action Enter the port list values without any wildcards.

Severity ERROR

SEC-1041

Message `<timestamp>, [SEC-1041], <sequence-number>,, ERROR, <system-name>, Invalid port member <port member> in portlist (<port list>). <Reason>.`

Probable Cause Indicates the port member is invalid for one of the following reasons:

- The value is not a number.
- The value is too long. Valid numbers must be between one and three characters long.
- The value cannot be parsed due to invalid characters.

Recommended Action Use valid syntax when entering the port members.

Severity ERROR

SEC-1042

Message `<timestamp>, [SEC-1042], <sequence-number>,, ERROR, <system-name>, Invalid index/area member <port member> in portlist (<Port list>). Out of range (<Minimum value> - <Maximum value>).`

Probable Cause Indicates the specified index or area member is not within the minimum and maximum range.

Recommended Action Use valid syntax when entering index or area numbers.

Severity ERROR

SEC-1043

Message `<timestamp>, [SEC-1043], <sequence-number>,, ERROR, <system-name>, Invalid port range <Minimum> - <Maximum>.`

Probable Cause Indicates the specified port is not within the minimum and maximum range.

Recommended Action Use valid syntax when entering port ranges.

Severity ERROR

SEC-1044

Message `<timestamp>, [SEC-1044], <sequence-number>,, ERROR, <system-name>, Duplicate member <member ID> in (<List>).`

Probable Cause Indicates the specified member is a duplicate in the input list. The list can be a policy list or a switch member list.

Recommended Action Do not specify any duplicates.

Severity ERROR

SEC-1045

Message `<timestamp>, [SEC-1045], <sequence-number>,, ERROR, <system-name>, Too many port members.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1046

Message `<timestamp>, [SEC-1046], <sequence-number>,, ERROR, <system-name>, Empty list.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1049

Message `<timestamp>, [SEC-1049], <sequence-number>,, ERROR, <system-name>, Invalid switch name <switch name>.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1050

Message `<timestamp>, [SEC-1050], <sequence-number>,, ERROR, <system-name>, There are more than one switches with the same name <switch name> in the fabric.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1051

Message `<timestamp>, [SEC-1051], <sequence-number>,, ERROR, <system-name>, Missing brace for port list <port list>.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1052

Message `<timestamp>, [SEC-1052], <sequence-number>,, ERROR, <system-name>, Invalid input.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1053

Message `<timestamp>, [SEC-1053], <sequence-number>,, ERROR, <system-name>, Invalid pFCS list <pFCS list>`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1054

Message `<timestamp>, [SEC-1054], <sequence-number>,, ERROR, <system-name>, Invalid FCS list length <list length>`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1055

Message `<timestamp>, [SEC-1055], <sequence-number>,, ERROR, <system-name>, Invalid FCS list <WWN list>`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1056

Message `<timestamp>, [SEC-1056], <sequence-number>,, ERROR, <system-name>, Invalid position <New position>. Only <Number of members in FCS list> members in list.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1057

Message `<timestamp>, [SEC-1057], <sequence-number>,, ERROR, <system-name>, No change. Both positions are the same.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1059

Message `<timestamp>, [SEC-1059], <sequence-number>,, ERROR, <system-name>, Fail to <operation, e.g., save, delete, etc.,> <named item> to flash.`

Probable Cause Indicates the operation failed when writing to flash.

Recommended Action Run the **supportFtp - e** command to FTP files from the switch and remove them from the flash.

Severity ERROR

SEC-1062

Message `<timestamp>, [SEC-1062], <sequence-number>,, ERROR, <system-name>, Invalid number of Domains in Domain List.`

Probable Cause Indicates that either no domains or domains more than the maximum number supported are specified.

Recommended Action Enter the correct number of domains.

Severity ERROR

SEC-1063

Message `<timestamp>, [SEC-1063], <sequence-number>,, ERROR, <system-name>, Failed to reset statistics.`

Probable Cause Indicates that either the type or domains specified are invalid.

Recommended Action Enter valid input.

Severity ERROR

SEC-1064

Message `<timestamp>, [SEC-1064], <sequence-number>,, ERROR, <system-name>, Failed to sign message.`

Probable Cause Indicates the public key infrastructure (PKI) objects on the switch are not in a valid state and the signature operation failed.

Recommended Action Run the **pkiShow** command to verify that all PKI objects are valid. If PKI objects are not valid, generate the PKI objects and install the certificate by following the field upgrade process.

Severity ERROR

SEC-1065

Message `<timestamp>, [SEC-1065], <sequence-number>,, ERROR, <system-name>, Invalid character in list.`

Probable Cause Indicates the input list has an invalid character.

Recommended Action Enter valid input.

Severity ERROR

SEC-1069

Message `<timestamp>, [SEC-1069], <sequence-number>,, ERROR, <system-name>, Security Database is corrupted.`

Probable Cause Indicates the security database is corrupted for unknown reasons.

Recommended Action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1071

Message `<timestamp>, [SEC-1071], <sequence-number>,, ERROR, <system-name>, No new security policy data to apply.`

Probable Cause Indicates that no changes in the defined security policy database need to be activated at this time.

Recommended Action Verify that the security event was planned. First change some policy definitions, then run the **secPolicyActivate** command to activate the policies.

Severity ERROR

SEC-1072

Message `<timestamp>, [SEC-1072], <sequence-number>,, ERROR, <system-name>, <Policy type> Policy List is Empty!`

Probable Cause Indicates the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended Action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1073

Message `<timestamp>, [SEC-1073], <sequence-number>,, ERROR, <system-name>, No FCS policy in list!`

Probable Cause Indicates the specific policy type is empty. The security database is corrupted for unknown reasons.

Recommended Action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1074

Message `<timestamp>, [SEC-1074], <sequence-number>,, ERROR, <system-name>, Cannot execute the command on this switch. Please check the secure mode and FCS status.`

Probable Cause Indicates a security command was run on a switch that is not allowed to run it either because it is in non-secure mode or because it does not have the required fabric configuration server (FCS) privilege.

Recommended Action If a security operation that is not allowed in non-secure mode is attempted, do not perform the operation in non-secure mode. In secure mode, run the command from a switch that has required privilege, that is, either a backup FCS or primary FCS.

Severity ERROR

SEC-1075

Message

```
<timestamp>, [SEC-1075], <sequence-number>,, ERROR, <system-name>, Fail to
<operation> new policy set on all switches.
```

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1076

Message

```
<timestamp>, [SEC-1076], <sequence-number>,, ERROR, <system-name>,
NoNodeWWNZoning option has been changed.
```

Probable Cause Indicates the NoNodeWWNZoning option has been changed. If the option is turned on, a zone member can be added using node WWNs, but the member will not be able to communicate with others nodes in the zone.

Recommended Action Re-enable the current zone configuration for the change to take effect.

Severity ERROR

SEC-1077

Message

```
<timestamp>, [SEC-1077], <sequence-number>,, ERROR, <system-name>, Failed to
activate new policy set on all switches.
```

Probable Cause Indicates the policy could not be activated. Possible reasons that the policy could not be activated include not enough memory or a busy switch.

Recommended Action Run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. Retry the command when all switches are ready.

Severity ERROR

SEC-1078

Message `<timestamp>, [SEC-1078], <sequence-number>,, ERROR, <system-name>, No new data to abort.`

Probable Cause Indicates there are no new changes in the defined security policy database that can be aborted.

Recommended Action Verify the security event was planned. Verify if there were really any changes to the defined policy database that can be aborted.

Severity ERROR

SEC-1079

Message `<timestamp>, [SEC-1079], <sequence-number>,, ERROR, <system-name>, The policy name <policy name> is invalid.`

Probable Cause Indicates the policy name entered in the **secPolicyCreate|Activate|Add|Delete** command was invalid.

Recommended Action Run the command again using a valid policy name.

Severity ERROR

SEC-1080

Message `<timestamp>, [SEC-1080], <sequence-number>,, ERROR, <system-name>, Operation denied. Please, use secModeEnable command.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1081

Message `<timestamp>, [SEC-1081], <sequence-number>,, ERROR, <system-name>, Entered a name for a DCC policy ID that was not unique.`

Probable Cause Indicates the device connection control (DCC) policy name given in the **secPolicyCreate** command was the same as another DCC policy.

Recommended Action Make sure that the DCC policy name has a unique alphanumeric string, and run the **secPolicyCreate** command again.

Severity ERROR

SEC-1082

Message `<timestamp>, [SEC-1082], <sequence-number>,, ERROR, <system-name>, Failed to create <policy name> policy.`

Probable Cause Indicates the security policy was not created due to faulty input or low resources.

Recommended Action Use proper syntax when creating policies. If the security database is too large, you must delete other members within the database before adding new members to a policy.

Severity ERROR

SEC-1083

Message `<timestamp>, [SEC-1083], <sequence-number>,, ERROR, <system-name>, Name already exists.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1084

Message `<timestamp>, [SEC-1084], <sequence-number>,, ERROR, <system-name>, Name exists for different type <Policy name>.`

Probable Cause Indicates the specified policy already exists.

Recommended Action No action is required.

Severity ERROR

SEC-1085

Message `<timestamp>, [SEC-1085], <sequence-number>,, ERROR, <system-name>, Failed to create <policy name>.`

Probable Cause Indicates that the security policy was not created.

Recommended Action Check that the current policy configuration is valid. For example, the RSNMP policy cannot exist without the WSNMP policy.

Severity ERROR

SEC-1086

Message `<timestamp>, [SEC-1086], <sequence-number>,, ERROR, <system-name>, The security database is too large to fit in flash.`

Probable Cause Indicates the security database has more data than the flash can accommodate.

Recommended Action Reduce the number of entries in some policies to decrease the security database size.

Severity ERROR

SEC-1087

Message `<timestamp>, [SEC-1087], <sequence-number>,, ERROR, <system-name>, The security database is larger than the data distribution limit of fabric <fabric data distribution limit> bytes.`

Probable Cause Indicates the security database has more data than can be distributed to some of the switches in the fabric.

Recommended Action Reduce the number of entries in the security policies to decrease the security database size.

Severity ERROR

SEC-1088

Message `<timestamp>, [SEC-1088], <sequence-number>,, ERROR, <system-name>, Cannot execute the command. Please try later.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1089

Message `<timestamp>, [SEC-1089], <sequence-number>,, ERROR, <system-name>, Policy name <policy name> was not found.`

Probable Cause Indicates the security policy name in the **secPolicyAdd** command does not exist.

Recommended Action Create the appropriate security policy first, then use its name in the **secPolicyAdd** command to add new members.

Severity ERROR

SEC-1090

Message `<timestamp>, [SEC-1090], <sequence-number>,, ERROR, <system-name>, SCC list contains FCS member. Please remove member from the FCS policy first.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1091

Message `<timestamp>, [SEC-1091], <sequence-number>,, ERROR, <system-name>, No policy to remove.`

Probable Cause Indicates the specified policy member does not exist or the policy itself does not exist.

Recommended Action Verify that the security policy name or member ID is correct.

Severity ERROR

SEC-1092

Message `<timestamp>, [SEC-1092], <sequence-number>,, ERROR, <system-name>, <Policy name> Name not found.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1093

Message `<timestamp>, [SEC-1093], <sequence-number>,, ERROR, <system-name>, New FCS list must have at least one member in common with current FCS list.`

Probable Cause Indicates the new fabric configuration server (FCS) list does not have a common member with the existing FCS list.

Recommended Action Resubmit the command with at least one member of the new FCS list in common with the current FCS list.

Severity ERROR

SEC-1094

Message `<timestamp>, [SEC-1094], <sequence-number>,, ERROR, <system-name>, Policy member not found.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1095

Message `<timestamp>, [SEC-1095], <sequence-number>,, ERROR, <system-name>, Deleting FCS policy is not allowed.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1096

Message

```
<timestamp>, [SEC-1096], <sequence-number>,, ERROR, <system-name>, Failed to
delete <policy name> because <reason text>.
```

Probable Cause Indicates a policy cannot be removed because deleting it would result in invalid security policy configuration.

Recommended Action Verify the security policy configuration requirements and remove any policies that require the policy you want to remove first.

Severity ERROR

SEC-1097

Message

```
<timestamp>, [SEC-1097], <sequence-number>,, ERROR, <system-name>, Cannot find
<active or defined> policy set.
```

Probable Cause Indicates the specified policy could not be found.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1098

Message

```
<timestamp>, [SEC-1098], <sequence-number>,, ERROR, <system-name>, No <active or
defined> FCS list.
```

Probable Cause Indicates the specified policy could not be found.

Recommended Action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1099

Message `<timestamp>, [SEC-1099], <sequence-number>,, ERROR, <system-name>, Please enable your switch before running secModeEnable.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1100

Message `<timestamp>, [SEC-1100], <sequence-number>,, ERROR, <system-name>, FCS switch present. Command terminated.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1101

Message `<timestamp>, [SEC-1101], <sequence-number>,, ERROR, <system-name>, Failed to enable security on all switches. Please retry later.`

Probable Cause Indicates the security enable failed on the fabric because one or more switches in the fabric are busy.

Recommended Action Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity ERROR

SEC-1102

Message `<timestamp>, [SEC-1102], <sequence-number>,, ERROR, <system-name>, Fail to download <security data>.`

Probable Cause Indicates the switch failed to download a certificate, security database, or policies. This can happen when the switch does not have enough resources to complete the operation, the fabric has not stabilized, or the policy database is an invalid format.

Recommended Action Wait for fabric to become stable and then retry the operation. If the policy database is in an illegal format (with **configDownload**), correct the format and retry the operation.

Severity ERROR

SEC-1104

Message `<timestamp>, [SEC-1104], <sequence-number>,, ERROR, <system-name>, Fail to get primary <Certificate or public key>.`

Probable Cause Indicates the switch failed to get either the primary certificate or a primary public key.

Recommended Action Verify the primary switch has a valid certificate installed and retry the operation. If a valid certificate is not installed, install a certificate by following the procedure specified in the *Secure Fabric OS Administrator's Guide*.

Severity ERROR

SEC-1105

Message `<timestamp>, [SEC-1105], <sequence-number>,, ERROR, <system-name>, Fail to disable secure mode on all switches.`

Probable Cause Indicates the switch failed to disable security in the fabric. This could happen if the switch cannot get the required resources to complete the command, and sending to a remote domain fails or the remote domain returns an error.

Recommended Action Run the **secFabricShow** to verify that all switches in the fabric are in the ready state. Retry the command when all switches are READY.

Severity ERROR

SEC-1106

Message `<timestamp>, [SEC-1106], <sequence-number>,, ERROR, <system-name>, Failed to sign message data.`

Probable Cause Indicates that some public key infrastructure (PKI) objects on the switch are not in a valid state, and a signature operation failed.

Recommended Action Run the **pkiShow** command and verify that all PKI objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *Secure Fabric OS Administrator's Guide*.

Severity ERROR

SEC-1107

Message `<timestamp>, [SEC-1107], <sequence-number>,, INFO, <system-name>, Stamp is 0.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1108

Message `<timestamp>, [SEC-1108], <sequence-number>,, ERROR, <system-name>, Fail to reset stamp on all switches.`

Probable Cause Indicates that a version reset operation failed either because the switch could not get all the required resources to perform the operation or because it failed to send the message to all switches in the fabric.

Recommended Action Verify that the security event was planned. If the security event was planned, run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity ERROR

SEC-1110

Message `<timestamp>, [SEC-1110], <sequence-number>,, ERROR, <system-name>, FCS list must be the first entry in the [Defined Security policies] section. Fail to download defined database.`

Probable Cause Indicates that a security policy download is attempted with a defined policy that does not have the fabric configuration server (FCS) policy as the first policy. The FCS policy is required to be the first policy in the defined security database.

Recommended Action Download a correct configuration with the fabric configuration server (FCS) policy as the first policy in the defined security database.

Severity ERROR

SEC-1111

Message `<timestamp>, [SEC-1111], <sequence-number>,, ERROR, <system-name>, New defined FCS list must have at least one member in common with current active FCS list. Fail to download defined database.`

Probable Cause Indicates the defined and active fabric configuration server (FCS) policy list failed to have at least one member in common.

Recommended Action A new FCS policy list must have at least one member in common with the previous FCS policy.

Severity ERROR

SEC-1112

Message `<timestamp>, [SEC-1112], <sequence-number>,, ERROR, <system-name>, FCS list must be the first entry in the Active Security policies, and the same as the current active FCS list in the switch.`

Probable Cause Indicates that either a security policy download is attempted with an active policy that does not have the fabric configurations server (FCS) policy as the first policy or the FCS policy is not same as the current FCS policy on the switch.

Recommended Action Make sure that the new FCS policy is the same as the current FCS policy on the switch.

Severity ERROR

SEC-1113

Message `<timestamp>, [SEC-1113], <sequence-number>,, WARNING, <system-name>, <Key> [ <Feature> license ] going to expire in <Expiry_days> days.`

Probable Cause Indicates the license period will expire soon.

Recommended Action Get a new license for this feature.

Severity WARNING

SEC-1114

Message `<timestamp>, [SEC-1114], <sequence-number>,, WARNING, <system-name>, <Key> [ <Feature> license ] has expired.`

Probable Cause Indicates the license period has expired.

Recommended Action Get a new license for this feature.

Severity WARNING

SEC-1115

Message `<timestamp>, [SEC-1115], <sequence-number>,, ERROR, <system-name>, No primary FCS to failover.`

Probable Cause Indicates that during an attempted **secFcsFailover**, no primary fabric configurations server (FCS) is present in the fabric.

Recommended Action Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity ERROR

SEC-1116

Message `<timestamp>, [SEC-1116], <sequence-number>,, ERROR, <system-name>, Fail to commit failover.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1117

Message `<timestamp>, [SEC-1117], <sequence-number>,, INFO, <system-name>, Fail to set <data>.`

Probable Cause Indicates the switch failed to save the data received by the primary fabric configuration server (FCS) switch. This data can be an FCS password, a non-FCS password, SNMP data, or multiple user authentication data.

Recommended Action Run the **secFabricShow** command to verify that all switches in the fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity INFO

SEC-1118

Message `<timestamp>, [SEC-1118], <sequence-number>,, INFO, <system-name>, Fail to set SNMP string.`

Probable Cause Indicates the SNMP string could not be set.

Recommended Action Usually this problem is transient. Retry the command.

Severity INFO

SEC-1119

Message `<timestamp>, [SEC-1119], <sequence-number>,, INFO, <system-name>, Secure mode has been enabled.`

Probable Cause Indicates the secure Fabric OS was enabled by the **secModeEnable** command.

Recommended Action Verify the security event was planned. If the security event was planned, there is no action required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1121

Message `<timestamp>, [SEC-1121], <sequence-number>,, ERROR, <system-name>, Time is out of range when <text>.`

Probable Cause Indicates the time on the switch is not synchronized with the primary fabric configuration server (FCS), the data packet is corrupted, or a replay attack is launched on the switch.

Recommended Action Verify the security event was planned. If the security event was planned, verify that all switches in the fabric are in time synchronization with the primary FCS and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1122

Message `<timestamp>, [SEC-1122], <sequence-number>,, INFO, <system-name>, Error code: <Domain ID>, <Error message>.`

Probable Cause Indicates that one of the switches in the fabric could not communicate with the primary fabric configuration server (FCS).

Recommended Action Run the **secFabricShow** command to verify that all switches in fabric are in the ready state. When all switches are in the ready state, retry the operation.

Severity INFO

SEC-1123

Message `<timestamp>, [SEC-1123], <sequence-number>,, INFO, <system-name>, Security database downloaded by Primary FCS.`

Probable Cause Indicates the security database was successfully downloaded from the primary fabric configuration server (FCS).

Recommended Action No action is required.

Severity INFO

SEC-1124

Message `<timestamp>, [SEC-1124], <sequence-number>,, INFO, <system-name>, Secure Mode is off.`

Probable Cause Indicates that a secure mode disable is attempted in a non-secure fabric.

Recommended Action No action is required.

Severity INFO

SEC-1126

Message `<timestamp>, [SEC-1126], <sequence-number>,, INFO, <system-name>, Secure mode has been disabled.`

Probable Cause Indicates that a secure mode disable operation completed successfully.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1130

Message `<timestamp>, [SEC-1130], <sequence-number>,, INFO, <system-name>, The Primary FCS has failed over to a new switch.`

Probable Cause Indicates an FCS failover operation was completed successfully.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1135

Message `<timestamp>, [SEC-1135], <sequence-number>,, INFO, <system-name>, Secure fabric version stamp has been reset.`

Probable Cause Indicates the version stamp of the secure fabric is reset.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1136

Message `<timestamp>, [SEC-1136], <sequence-number>,, ERROR, <system-name>, Failed to verify signature <data type, MUA, policy, etc.,>.`

Probable Cause Indicates the receiving switch fails to validate the security database sent from the primary fabric configuration server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity ERROR

SEC-1137

Message `<timestamp>, [SEC-1137], <sequence-number>,, ERROR, <system-name>, No signature in <data type, MUA, policy, etc.,>.`

Probable Cause Indicates the receiving switch fails to validate the security database sent from the primary fabric configurations server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity ERROR

SEC-1138

Message `<timestamp>, [SEC-1138], <sequence-number>,, INFO, <system-name>, Security database download received from Primary FCS.`

Probable Cause Indicates that a non-primary fabric configuration server (FCS) switch received a security database download.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1139

Message `<timestamp>, [SEC-1139], <sequence-number>,, ERROR, <system-name>, The RSNMP_POLICY cannot exist without the WSNMP_POLICY.`

Probable Cause Indicates that the receiving switch failed to validate the security database sent from the primary fabric configuration server (FCS) switch. This message usually indicates that the data package is corrupted, the time stamp on the package is out of range as a result of a replay attack or out-of-sync time service, or the signature verification failed. Signature verification failure indicates either an internal error (such as losing the primary public key) or an invalid database.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that switch. This message might also be the result of an internal corruption or a hacker attack to the secure fabric.

Severity ERROR

SEC-1142

Message `<timestamp>, [SEC-1142], <sequence-number>,, INFO, <system-name>, Reject new policies. <reason text>.`

Probable Cause Indicates the new polices are rejected due to the reason specified.

Recommended Action Use proper syntax when entering policy information.

Severity INFO

SEC-1145

Message `<timestamp>, [SEC-1145], <sequence-number>,, INFO, <system-name>, A security admin event has occurred. This message is for information purpose only. The message for individual event is: <Event specific data>`

Probable Cause Indicates one of the following has occurred:

- The names for the specified policies have changed.
- The passwords have changed for the specified accounts.
- The SNMP community strings have been changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1146

Message `<timestamp>, [SEC-1146], <sequence-number>,, INFO, <system-name>, PID changed: <State>.`

Probable Cause Indicates the PID format of the switch was changed either to extended-edge PID or from extended-edge PID. If the device connection control (DCC) polices existed, all index/area ID values either increased or decreased by 16. The values wrap around after 128. If a DCC policy contains an index/area of 127 before changing to extended-edge PID, then the new index/area is 15, because of the wraparound.

Recommended Action No action is required.

Severity INFO

SEC-1153

Message `<timestamp>, [SEC-1153], <sequence-number>,, INFO, <system-name>, Error in RCA: RCS is not supported`

Probable Cause Indicates that reliable commit service (RCS) is not supported.

Recommended Action Run the **rcsInfoShow** command to view RCS capability on the fabric. RCS must be capable on all switches in the fabric to be enabled. If all switches are capable, it is automatically enabled.

For any switch that does not support RCS, obtain the latest firmware version from your switch supplier, and run the **firmwareDownload** command to upgrade the firmware.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

SEC-1154

Message `<timestamp>, [SEC-1154], <sequence-number>,, INFO, <system-name>, PID change failed: <Reason> <defined status> <active status>.`

Probable Cause Indicates that either the defined or the active policy could not be updated. If the policy database is very large, it might not be able to change the index/area because the new policy database exceeds the maximum size. This message can also be caused when the switch is short of memory. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action Reduce the size of the policy database.

Severity INFO

SEC-1155

Message

```
<timestamp>, [SEC-1155], <sequence-number>,, INFO, <system-name>, PID change
failed: <Reason> <defined status> <active status>.
```

Probable Cause Indicates that either the defined or active policy was too large after modifying the index/area ID. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action Reduce the size of the specified policy database.

Severity INFO

SEC-1156

Message

```
<timestamp>, [SEC-1156], <sequence-number>,, INFO, <system-name>, Change failed:
<Reason> <defined status> <active status>.
```

Probable Cause Indicates the security daemon is busy. The status values can be defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action For the first reject, wait a few minutes and then resubmit the transaction. Fabric-wide commands might take a few minutes to propagate throughout the fabric. Make sure to wait a few minutes between executing commands so that your commands do not overlap in the fabric.

Severity INFO

SEC-1157

Message

```
<timestamp>, [SEC-1157], <sequence-number>,, INFO, <system-name>, PID Change
failed: <Reason> <defined status> <active status>.
```

Probable Cause Indicates the provisioning resources for a security policy failed due to low memory or internal error. The status values can be either defined, active, or both. A negative value means that a policy set was failed by the daemon.

Recommended Action Retry the failed command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

SEC-1158

Message `<timestamp>, [SEC-1158], <sequence-number>,, INFO, <system-name>, Invalid name <Policy or Switch name>.`

Probable Cause Indicates the specified name is invalid. The name can be a policy name or a switch name.

Recommended Action Enter a valid name.

Severity INFO

SEC-1159

Message `<timestamp>, [SEC-1159], <sequence-number>,, INFO, <system-name>, Non_Reachable domain <Domain ID>.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1160

Message `<timestamp>, [SEC-1160], <sequence-number>,, INFO, <system-name>, Duplicate port <port ID> in port list (<port list>).`

Probable Cause Indicates a duplicate port member exists in the specified port list.

Recommended Action Verify that there is no duplicate member in the port list.

Severity INFO

SEC-1163

Message `<timestamp>, [SEC-1163], <sequence-number>,, ERROR, <system-name>, System is already in secure mode. Lockdown option cannot be applied.`

Probable Cause Indicates the lockdown option was attempted while the fabric is already in secure mode.

Recommended Action Do not use lockdown option with the **secModeEnable** command when a switch is already in secure mode.

Severity ERROR

SEC-1164

Message
```
<timestamp>, [SEC-1164], <sequence-number>,, ERROR, <system-name>, Lockdown
option cannot be applied on a non-FCS switch.
```

Probable Cause Indicates the attempt to enable security is made on a switch that is not present in the fabric configuration server (FCS) list.

Recommended Action Add the switch to the FCS policy list when using the lockdown option to enable security.

Severity ERROR

SEC-1165

Message
```
<timestamp>, [SEC-1165], <sequence-number>,, ERROR, <system-name>, Low memory,
failed to enable security on all switches.
```

Probable Cause Indicates the system is low on memory.

Recommended Action Wait a few minutes and try the command again.

Severity ERROR

SEC-1166

Message
```
<timestamp>, [SEC-1166], <sequence-number>,, ERROR, <system-name>, Non FCS tries
to commit failover.
```

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1167

Message `<timestamp>, [SEC-1167], <sequence-number>,, ERROR, <system-name>, Another FCS failover is in process. Command terminated.`

Probable Cause Indicates that because another failover is already in progress, this failover attempt cannot proceed.

Recommended Action Verify the security event was planned. If the security event was planned, retry fabric configurations server (FCS) failover after current failover has completed, if this switch should become primary FCS. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity ERROR

SEC-1168

Message `<timestamp>, [SEC-1168], <sequence-number>,, ERROR, <system-name>, Primary FCS failover is busy. Please retry later.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configurations server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity ERROR

SEC-1170

Message `<timestamp>, [SEC-1170], <sequence-number>,, INFO, <system-name>, This command must be executed on the Primary FCS switch, the first reachable switch in the FCS list.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1171

Message `<timestamp>, [SEC-1171], <sequence-number>,, ERROR, <system-name>, Disabled secure mode due to invalid security object.`

Probable Cause Indicates the switch is segmented, and secure mode is disabled on the switch because there was no license present or no public key infrastructure (PKI) objects.

Recommended Action Run the **pkiShow** command to determine whether all PKI objects exist. If they do not exist, run the **pkiCreate** command to create them for the switch.

Run the **licenseAdd** command to install the required license key. Refer to your switch supplier to obtain a license if you do not have one.

Severity ERROR

SEC-1172

Message `<timestamp>, [SEC-1172], <sequence-number>,, ERROR, <system-name>, Failed to identify role.`

Probable Cause Indicates the switch is unable to determine its role (primary FCS or backup FCS) in the secure fabric.

Recommended Action Verify all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1173

Message `<timestamp>, [SEC-1173], <sequence-number>,, ERROR, <system-name>, Lost contact with Primary FCS switch.`

Probable Cause Indicates the switch has lost contact with the primary fabric configuration server (FCS) switch in the secure fabric. This could be due to the primary FCS being disabled.

Recommended Action If the primary FCS was disabled intentionally, no action is required; if not, check the primary FCS.

Severity ERROR

SEC-1174

Message `<timestamp>, [SEC-1174], <sequence-number>,, ERROR, <system-name>, Failed to set <FCS or non-FCS> password.`

Probable Cause Indicates the FCS or non-FCS password could not be set.

Recommended Action Verify all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1175

Message `<timestamp>, [SEC-1175], <sequence-number>,, ERROR, <system-name>, Failed to install zone data.`

Probable Cause Indicates the zone database could not be installed on the switch.

Recommended Action Verify all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1176

Message `<timestamp>, [SEC-1176], <sequence-number>,, ERROR, <system-name>, Failed to generate new version stamp.`

Probable Cause Indicates the primary fabric configuration server (FCS) failed to generate a new version stamp due to the fabric not being stable.

Recommended Action Verify all switches in the fabric are in time synchronization with the primary and that no external entity is trying to access the fabric. When verification is complete, retry the operation.

Severity ERROR

SEC-1180

Message `<timestamp>, [SEC-1180], <sequence-number>,, INFO, <system-name>, Added account <user name> with <role name> authorization.`

Probable Cause Indicates the specified new account has been created.

Recommended Action No action is required.

Severity INFO

SEC-1181

Message `<timestamp>, [SEC-1181], <sequence-number>,, INFO, <system-name>, Deleted account <user name>`

Probable Cause Indicates the specified account has been deleted.

Recommended Action No action is required.

Severity INFO

SEC-1182

Message `<timestamp>, [SEC-1182], <sequence-number>,, INFO, <system-name>, Recovered <number of> accounts.`

Probable Cause Indicates the specified number of accounts has been recovered from backup.

Recommended Action No action is required.

Severity INFO

SEC-1183

Message `<timestamp>, [SEC-1183], <sequence-number>,, ERROR, <system-name>, Policy to binary conversion error: Port <port number> is out range.`

Probable Cause Indicates a security database conversion has failed because of an invalid value.

Recommended Action Retry the command with a valid value.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1184

Message `<timestamp>, [SEC-1184], <sequence-number>,, INFO, <system-name>, <server> configuration change, action <action>, server ID <server>.`

Probable Cause Indicates the specified action is applied to the specified Remote Authentication Dial-in User Service (RADIUS) / Lightweight Directory Access Protocol (LDAP) server configuration. The possible actions are ADD, REMOVE, CHANGE, and MOVE

Recommended Action No action is required.

Severity INFO

SEC-1185

Message `<timestamp>, [SEC-1185], <sequence-number>,, INFO, <system-name>, <action> switch DB.`

Probable Cause Indicates the switch database was enabled or disabled as the secondary authentication, accounting, and authorization (AAA) mechanism when the Remote Authentication Dial-in User Service (RADIUS) / Lightweight Directory Access Protocol (LDAP) is the primary AAA mechanism

Recommended Action No action is required.

Severity INFO

SEC-1186

Message `<timestamp>, [SEC-1186], <sequence-number>,, INFO, <system-name>, <action> <action> Configuration.`

Probable Cause Indicates the remote authentication dial-in user service (RADIUS/LDAP) configuration was enabled or disabled as the primary authentication, accounting, and authorization (AAA) mechanism.

Recommended Action No action is required.

Severity INFO

SEC-1187

Message `<timestamp>, [SEC-1187], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized switch <switch WWN> tries to join fabric.`

Probable Cause Indicates a switch connection control (SCC) security violation was reported. The specified unauthorized switch attempts to join the fabric.

Recommended Action Check the switch connection control policy (SCC) policy to verify the switches allowed in the fabric. If the switch should be allowed in the fabric but it is not included in the SCC policy, add the switch to the policy. If the switch is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1188

Message `<timestamp>, [SEC-1188], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized device <device node name> tries to FLOGI to index/area <port number> of switch <switch WWN>.`

Probable Cause Indicates a device connection control (DCC) security violation was reported. The specified device attempted to login using fabric login (FLOGI) to an unauthorized port. The DCC policy correlates specific devices to specific port locations. If the device changes connected port, the device will not be allowed to login.

Recommended Action Check the DCC policy and verify the specified device is allowed in the fabric and is included in the DCC policy. If the specified device is not included in the policy, add it to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1189

Message `<timestamp>, [SEC-1189], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized host with IP address <IP address> tries to do SNMP write operation.`

Probable Cause Indicates an SNMP security violation was reported. The specified unauthorized host attempted to perform a write SNMP operation.

Recommended Action Check the WSNMP policy and verify which hosts are allowed access to the fabric through SNMP. If the host is allowed access to the fabric but is not included in the policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1190

Message `<timestamp>, [SEC-1190], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized host with IP address <IP address> tries to do SNMP read operation.`

Probable Cause Indicates an SNMP security violation was reported. The specified unauthorized host attempted to perform a read SNMP operation.

Recommended Action Check the RSNMP policy to verify the hosts allowed access to the fabric through SNMP read operations are included in the RSNMP policy. If the host is allowed access but is not included in the RSNMP policy, add the host to the policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1191

Message `<timestamp>, [SEC-1191], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized host with IP address <Ip address> tries to establish HTTP connection.`

Probable Cause Indicates an HTTP security violation was reported. The specified unauthorized host attempted to establish an HTTP connection.

Recommended Action Determine whether the host IP address specified in the message can be used to manage the fabric through an HTTP connection. If so, add the host IP address to the HTTP policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1192

Message `<timestamp>, [SEC-1192], <sequence-number>,, INFO, <system-name>, Security violation: Login failure attempt via <connection method>.`

Probable Cause Indicates a serial or modem login security violation was reported. An incorrect password was used while trying to log in through a serial or modem connection; the login failed.

Recommended Action Use the correct password.

Severity INFO

SEC-1193

Message `<timestamp>, [SEC-1193], <sequence-number>,, INFO, <system-name>, Security violation: Login failure attempt via <connection method>. IP Addr: <IP address>`

Probable Cause Indicates a specified login security violation was reported. The incorrect password was used while trying to log in through the specified connection method; the login failed.

Recommended Action The error message lists the violating IP address. Verify that this IP address is being used by a valid switch admin. Use the correct password.

Severity INFO

SEC-1194

Message `<timestamp>, [SEC-1194], <sequence-number>,, WARNING, <system-name>, This switch does not have all the required PKI objects correctly installed.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity WARNING

SEC-1195

Message `<timestamp>, [SEC-1195], <sequence-number>,, WARNING, <system-name>, This switch has no <component> license.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity WARNING

SEC-1196

Message `<timestamp>, [SEC-1196], <sequence-number>,, WARNING, <system-name>, Switch does not have all default account names.`

Probable Cause Indicates the default switch accounts admin and user do not exist on the switch when enabling security.

Recommended Action Reset the default admin and user account names on the switch that reported the warning and retry enabling security.

Severity WARNING

SEC-1197

Message `<timestamp>, [SEC-1197], <sequence-number>,, INFO, <system-name>, Changed account <user name>.`

Probable Cause Indicates the specified account has changed.

Recommended Action No action is required.

Severity INFO

SEC-1198

Message `<timestamp>, [SEC-1198], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized host with IP address <IP address> tries to establish API connection.`

Probable Cause Indicates an API security violation was reported. The specified unauthorized host attempted to establish an API connection.

Recommended Action Check to see if the host IP address specified in the message can be used to manage the fabric through an API connection. If so, add the host IP address to the API policy of the fabric. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1199

Message `<timestamp>, [SEC-1199], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized access to serial port of switch <switch instance>.`

Probable Cause Indicates a serial connection policy security violation was reported. An attempt was made to access the serial console on the specified switch instance when it is disabled.

Recommended Action Check to see if an authorized access attempt is being made on the console. If so, add the switch world wide name (WWN) to the serial policy. If the host is not allowed access to the fabric, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1200

Message `<timestamp>, [SEC-1200], <sequence-number>,, INFO, <system-name>, Security violation: MS command is forwarded from non-primary FCS switch.`

Probable Cause Indicates a management server (MS) forward security violation was reported. A management server command was forwarded from a non-primary fabric configuration server (FCS) switch.

Recommended Action Check the MS policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1201

Message `<timestamp>, [SEC-1201], <sequence-number>,, INFO, <system-name>, Security violation: MS device <device WWN> operates on non-primary FCS switch.`

Probable Cause Indicates a management server (MS) operation security violation was reported. An MS device operation occurred on a non-primary fabric configuration server (FCS) switch.

Recommended Action Check the management server policy and verify the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1202

Message `<timestamp>, [SEC-1202], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized access from MS device node name <device node name>, device port name <device port name>.`

Probable Cause Indicates a management server (MS) security violation was reported. The unauthorized device specified in the message attempted to establish a connection.

Recommended Action Check the MS server policy and verify that the connection is allowed. If the connection is allowed but not specified, enable the connection in the MS policy. If the MS policy does not allow the connection, this is a valid violation message and an unauthorized entity is trying to access your fabric. Take appropriate action, as defined by your enterprise security policy.

Severity INFO

SEC-1203

Message `<timestamp>, [SEC-1203], <sequence-number>,, INFO, <system-name>, Login information: Login successful via TELNET/SSH/RSH. IP Addr: <IP address>`

Probable Cause Indicates the IP address of the remote station logging in.

Recommended Action No action is required.

Severity INFO

SEC-1250

Message `<timestamp>, [SEC-1250], <sequence-number>,, WARNING, <system-name>, DCC enforcement API failed: <failed action> err=<status>, key=<data>`

Probable Cause Indicates an internal error caused the DCC policy enforcement to fail.

Recommended Action Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

SEC-1251

Message `<timestamp>, [SEC-1251], <sequence-number>,, ERROR, <system-name>, Policy to binary conversion error: <text message> <value>.`

Probable Cause Indicates the security database conversion failed because of invalid values. The reason is specified in the *text message* variable and a faulty value is printed in the *value* variable.

Recommended Action Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1253

Message

```
<timestamp>, [SEC-1253], <sequence-number>,, ERROR, <system-name>, Bad DCC
interface state during <Phase>, state=<state>.
```

Probable Cause Indicates an internal error has caused the device connection control (DCC) policy update to fail in the provision, commit, or cancel phases.

Recommended Action Retry the failed security command.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1300

Message

```
<timestamp>, [SEC-1300], <sequence-number>,, INFO, <system-name>, This switch is
in VcEncode mode. Security is not supported.
```

Probable Cause Indicates the switch is set up with VC-encoded mode.

Recommended Action Turn off VC-encoded mode before enabling security.

Severity INFO

SEC-1301

Message

```
<timestamp>, [SEC-1301], <sequence-number>,, INFO, <system-name>, This switch is
in interop mode. Security is not supported.
```

Probable Cause Indicates the switch is interop-mode enabled.

Recommended Action Disable interop-mode using the **interopMode** command before enabling the Secure Fabric OS feature.

Severity INFO

SEC-1302

Message `<timestamp>, [SEC-1302], <sequence-number>,, INFO, <system-name>, This switch does not have all the required PKI objects correctly installed.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify that the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1303

Message `<timestamp>, [SEC-1303], <sequence-number>,, INFO, <system-name>, This software version does not support security.`

Probable Cause Indicates the currently installed software version does not support the Brocade Secure Fabric OS feature.

Recommended Action Run the **firmwareDownload** command to update the firmware to the latest version for your specific switch. Verify the firmware you are installing supports the Brocade Secure Fabric OS feature.

Severity INFO

SEC-1304

Message `<timestamp>, [SEC-1304], <sequence-number>,, INFO, <system-name>, This switch has no security license.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1305

Message `<timestamp>, [SEC-1305], <sequence-number>,, INFO, <system-name>, This switch has no zoning license.`

Probable Cause Indicates there has been a corruption during the distribution of the security database. This can only occur when the primary fabric configuration server (FCS) is distributing the security database to the other switches in the fabric and local validation finds that there is an error in the security database. This is a rare occurrence.

Recommended Action Run the **secFabricShow** command to verify the fabric is still consistent. All the switches should be in the ready state. If a switch is in the error state, the database might not be correctly updated for that specific switch.

Severity INFO

SEC-1306

Message

```
<timestamp>, [SEC-1306], <sequence-number>,, INFO, <system-name>, Failed to
verify certificate with root CA.
```

Probable Cause Indicates the certificate could not be verified with root certificate authority (CA). This could happen if an unauthorized switch tries to access the fabric that is not certified by a trusted root CA or a root CA certificate does not exist on the switch.

Recommended Action Run the **pkiShow** command and verify that all public key infrastructure (PKI) objects exist on the switch. If a failure to validate PKI objects occurs, follow the steps for re-creating PKI objects outlined in the *Secure Fabric OS Administrator's Guide*. If PKI objects are valid, verify that an unauthorized switch is not trying to access the fabric.

Severity INFO

SEC-1307

Message

```
<timestamp>, [SEC-1307], <sequence-number>,, INFO, <system-name>, Got response
from <Radius/LDAP server identity> server <Radius/LDAP server identity>.
```

Probable Cause Indicates that after some servers timed out, the specified remote authentication dial-in user service (RADIUS/LDAP) server responded to a switch request.

Recommended Action If the message appears frequently, move the responding server to the top of the RADIUS/LDAP server configuration list using the **aaaConfig** command.

Severity INFO

SEC-1308

Message

```
<timestamp>, [SEC-1308], <sequence-number>,, INFO, <system-name>, All %s servers
have failed to respond.
```

Probable Cause Indicates that all servers in the remote authentication dial-in user service (RADIUS) configuration have failed to respond to a switch request within the specified time-out.

Recommended Action Verify the switch has proper network connectivity to the specified remote authentication dial-in user service (RADIUS) servers, and the servers are correctly configured.

Severity INFO

SEC-1309

Message `<timestamp>, [SEC-1309], <sequence-number>,, INFO, <system-name>, Waiting for RCS transaction to complete: <Wait time in seconds> secs`

Probable Cause Indicates that Secure Fabric OS is still waiting for the reliable commit service (RCS) transaction to complete.

Recommended Action Verify if there are any RCS or RTWR errors. If not, the transaction is still in progress.

Severity INFO

SEC-1310

Message `<timestamp>, [SEC-1310], <sequence-number>,, INFO, <system-name>, Unable to determine data distribution limit of fabric. Please retry later.`

Probable Cause Indicates the data distribution limit could not be obtained from all switches in the fabric. This may happen if the fabric is reconfiguring or a new domain joined the fabric.

Recommended Action Retry the command when the fabric is stable.

Severity INFO

SEC-1311

Message `<timestamp>, [SEC-1311], <sequence-number>,, ERROR, <system-name>, Security mode cannot be enabled because one or more of the password policies is not set to default value.`

Probable Cause Indicates the security enable failed on the fabric because one or more switches in the fabric have password policies that are not set to the default value.

Recommended Action Verify the security event was planned.

If the security event was planned, run the **passwdCfg --setDefault** command on each switch in the fabric to set the password policies to the default value. Then verify with **passwdCfg --show** that password policies are set to the default values on all switches and retry the **secModeEnable** command.

Severity ERROR

SEC-1312

Message `<timestamp>, [SEC-1312], <sequence-number>,, INFO, <system-name>, <MESG Message>.`

Probable Cause Indicates the **passwdCfg** parameters changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1313

Message
```
<timestamp>, [SEC-1313], <sequence-number>,, INFO, <system-name>, The passwdcfg
parameters were set to default values.
```

Probable Cause Indicates the **passwdCfg** parameters were set to default values.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1314

Message
```
<timestamp>, [SEC-1314], <sequence-number>,, ERROR, <system-name>, Reading <IP
Address Description > IP address from EM failed.
```

Probable Cause Indicates the call to the EM module to retrieve the IP address failed.

Recommended Action Restart the system to fix this error. If the problem persists contact your switch service provider.

Severity ERROR

SEC-1315

Message
```
<timestamp>, [SEC-1315], <sequence-number>,, ERROR, <system-name>, <Name of
command > command failed -<List of databases rejecting distribution > dbs
configured for rejection on this switch
```

Probable Cause Indicates there was an attempt to distribute databases to a switch that was configured not to accept distributions from the fabric.

Recommended Action Verify the accept distribution configuration for the listed databases. Use the **fddCfg** command to verify and correct the configuration if necessary.

Severity ERROR

SEC-1316

Message `<timestamp>, [SEC-1316], <sequence-number>,, WARNING, <system-name>, <Policy Name> policy is conflicting with domain <Domain Number>`

Probable Cause Indicates the newly added switches to the fabric, as specified by Domain Number, have a conflicting policy with the local switch.

Recommended Action Check the conflicting policy and make the new swithces and the local switch policies the same.

Severity WARNING

SEC-1317

Message `<timestamp>, [SEC-1317], <sequence-number>,, INFO, <system-name>, Inconsistent fabric, rejecting transaction`

Probable Cause Indicates that either this domain is performing FDD merge or matched domains are not the same as what CM sees.

Recommended Action If a policy conflict exists, resolve it, then wait for the fabric to become stable. Retry the distribution.

Severity INFO

SEC-1318

Message `<timestamp>, [SEC-1318], <sequence-number>,, INFO, <system-name>, Transaction rejected due to inconsistent fabric`

Probable Cause Indicates that some domains detected an inconsistent fabric.

Recommended Action Resolve the policy conflict, if there is one, then wait for the fabric to stabilize. Retry the distribution.

Severity INFO

SEC-1319

Message `<timestamp>, [SEC-1319], <sequence-number>,, INFO, <system-name>, <Event name> updated <Datasets updated> dbs(s)`

Probable Cause Indicates the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1320

Message `<timestamp>, [SEC-1320], <sequence-number>,, WARNING, <system-name>, Non-acl domain <Domain Number> tries to join a fabric with strict fabric wide policy`

Probable Cause Indicates that a domain not supporting an access control list (ACL) policy tried to join a fabric with a strict fabric-wide policy.

Recommended Action No action is required. The domain is denied by disallowing all its E_ports from connecting to the fabric.

Severity WARNING

SEC-1321

Message `<timestamp>, [SEC-1321], <sequence-number>,, ERROR, <system-name>, Failed secure mode enable command. Reason: <Reason>.`

Probable Cause Indicates the security enable failed on the fabric because the switch has a conflicting configuration such as fabric wide consistency configuration or AD configuration.

Recommended Action Verify the security event was planned.

If the security event was planned, run the **fddcfg --fabwideset ""** command or **ad --clear** command to clear the fabric wide consistency configuration or AD configuration and retry the **secModeEnable** command.

Severity ERROR

SEC-1322

Message `<timestamp>, [SEC-1322], <sequence-number>,, WARNING, <system-name>, Some DCC policy is too large, distribution cancelled`

Probable Cause Indicates this fabric is not able to support a device connection control (DCC) policy with more than 256 ports.

Recommended Action Reconfigure any policy that includes more than 256 ports in its member list, then save the policy configuration changes.

Severity WARNING

SEC-1323

Message `<timestamp>, [SEC-1323], <sequence-number>,, INFO, <system-name>, Keys \"<Key Name>\" ignored during configdownload.`

Probable Cause Indicates the specified key is ignored during **configDownload**.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1324

Message `<timestamp>, [SEC-1324], <sequence-number>,, INFO, <system-name>, Fabric transaction failure. RCS error: <Error code>`

Probable Cause Indicates the reliable commit service (RCS) transaction failed with the specified reason code.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1325

Message `<timestamp>, [SEC-1325], <sequence-number>,, ERROR, <system-name>, Security enforcement: Switch <switch WWN> connecting to port <Port number> is not authorized to stay in fabric.`

Probable Cause Indicates that because of a switch connection control (SCC) policy violation, the switch is being disabled on the specified port.

Recommended Action No action is required unless the switch must remain in the fabric. If the switch must remain in the fabric, add the switch world wide name (WWN) to the SCC policy, then attempt to join the switch with the fabric.

Severity ERROR

SEC-1326

Message `<timestamp>, [SEC-1326], <sequence-number>,, INFO, <system-name>, Event: fddcfg --fabwideset, Status: success, Info: Fabric wide configuration set to <Fabric-wide configuration set by user>.`

Probable Cause Indicates the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-1327

Message `<timestamp>, [SEC-1327], <sequence-number>,, WARNING, <system-name>, Strict <Policy Name> policy is conflicting with domain <Domain Number>`

Probable Cause Indicates the policy is conflicting with the domain.

Recommended Action No action is required. The domain is denied by disallowing all its E_ports connected to the fabric. If the domain should be allowed to merge with the fabric, then resolve the issue by making the conflicting policies the same.

Severity WARNING

SEC-1328

Message
```
<timestamp>, [SEC-1328], <sequence-number>,, ERROR, <system-name>, Attempt to
enable secure mode failed. Reason: <Reason>.
```

Probable Cause Indicates the **secModeEnable** command failed on the fabric because Authentication Policy is enabled on the switch.

Recommended Action Verify the security event was planned. If the security event was planned, run the **authUtil --policy passive** command to disable the Authentication Policy and retry the **secModeEnable** command.

Severity ERROR

SEC-1329

Message
```
<timestamp>, [SEC-1329], <sequence-number>,, ERROR, <system-name>, IPFilter
enforcement: Failed to enforce ipfilter policy of <policy Type> type because of
<Error code>.
```

Probable Cause Indicates the IP filter policy enforcement failed due to internal system failure.

Recommended Action Run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SEC-1330

Message
```
<timestamp>, [SEC-1330], <sequence-number>,, ERROR, <system-name>, <Name of
command> command failed - <List of databases rejecting distribution> db(s) are
coming from a non-Primary switch.
```

Probable Cause Indicates an attempt was made to distribute databases either from a backup fabric configuration server (FCS) switch or from a non-FCS switch.

Recommended Action Verify the distribution is initiated by the primary FCS switch. Use the **secPolicyShow** command to verify and correct the configuration if necessary.

Severity ERROR

SEC-1331

Message `<timestamp>, [SEC-1331], <sequence-number>,, ERROR, <system-name>, Attempt to enable secure mode failed. Reason: <Reason>.`

Probable Cause Indicates the **secModeEnable** command failed on the fabric because default IP Filter policies are not active on the switch, or an active transaction exists on IP Filter policies.

Recommended Action Verify the security event was planned. If the security event was planned, run the **ipfilter --activate default_ipv4** or the **ipfilter --activate default_ipv6** command to activate default IP Filter Policies. Use the **ipfilter --save** or the **ipfilter --transabort** commands to save or abort any active transaction on IP Filter policies. Then retry the **secModeEnable** command.

Severity ERROR

SEC-1332

Message `<timestamp>, [SEC-1332], <sequence-number>,, ERROR, <system-name>, Fabric wide policy is conflicting as <Policy Name> is present in the fabric wide policy and 5.3 or 5.2 switches present in the fabric.`

Probable Cause Indicates the fabric-wide policy is conflicting.

Recommended Action Remove either the FCS from the fabric-wide policy, or remove 5.3 and 5.2 switches from the fabric, or set the fabric-wide mode for FCS as Strict.

Severity ERROR

SEC-1333

Message `<timestamp>, [SEC-1333], <sequence-number>,, INFO, <system-name>, <Name of command> command failed. There are VF enabled switches in fabric. <List of databases rejecting distribution> db(s) distribution is blocked.`

Probable Cause Indicates an attempt to distribute PWD or IPFILTER databases from the fabric to a switch that is VF-enabled.

Recommended Action If the databases need to be distributed, disable VF on all the switches that have VF enabled. If the databases do not need to be distributed, no action is required.

Severity ERROR

SEC-3005

Message `<timestamp>, [SEC-3005], <sequence-number>, AUDIT, INFO, <system-name>, Event: <Event Name>, Status: success, Info: Added member(s) <Members added> to policy <Policy Name>.`

Probable Cause Indicates new members have been added to a security policy. If you use a wildcard (for example, an asterisk) in adding members to a policy, the audit report displays the wildcard in the event info field.

Recommended Action Verify the addition of members to the policy was planned. If the addition of members was planned, no action is required. If the addition of members was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3035

Message

```
<timestamp>, [SEC-3035], <sequence-number>, AUDIT, INFO, <system-name>, Event:
ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy(ies) saved.
```

Probable Cause Indicates that the specified IP filter policy has been saved.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3036

Message

```
<timestamp>, [SEC-3036], <sequence-number>, AUDIT, INFO, <system-name>, Event:
ipfilter, Status: failed, Info: Failed to save changes for <IP Filter Policy>
ipfilter policies.
```

Probable Cause Indicates that that the specified IP filter policy has not been saved.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3037

Message

```
<timestamp>, [SEC-3037], <sequence-number>, AUDIT, INFO, <system-name>, Event:
ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy activated.
```

Probable Cause Indicates that that the specified IP filter policy has been activated.

Recommended Action Verify that the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3038

Message `<timestamp>, [SEC-3038], <sequence-number>, AUDIT, INFO, <system-name>, Event: ipfilter, Status: failed, Info: Failed to activate <IP Filter Policy> ipfilter policy.`

Probable Cause Indicates that the specified IP filter policy failed to activate.

Recommended Action Verify that the security event was planned. If the event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3039

Message `<timestamp>, [SEC-3039], <sequence-number>, AUDIT, INFO, <system-name>, Event:Securty Violation , Status: failed, Info: Unauthorized host with IP address <IP address of the violating host> tries to establish connection using <Protocol Connection Type>.`

Probable Cause Indicates that a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the specified protocol connection.

Severity INFO

SEC-3050

Message `<timestamp>, [SEC-3050], <sequence-number>, AUDIT, INFO, <system-name>, Event: <Event Name>, Status: success, Info: <Event Specific Info>.`

Probable Cause Indicates the specified sshutil operation was performed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3051

Message `<timestamp>, [SEC-3051], <sequence-number>, AUDIT, INFO, <system-name>, The license key <key> is <Action>.`

Probable Cause Indicates that a license key is added or removed.

Recommended Action No action is required.

Severity INFO

SEC-3061

Message `<timestamp>, [SEC-3061], <sequence-number>, AUDIT, INFO, <system-name>, Role <role name> is created.`

Probable Cause Indicates a role name was created.

Recommended Action No action is required.

Severity INFO

SEC-3062

Message `<timestamp>, [SEC-3062], <sequence-number>, AUDIT, INFO, <system-name>, Role <role name> is deleted.`

Probable Cause Indicates a role name was deleted.

Recommended Action No action is required.

Severity INFO

SEC-3063

Message `<timestamp>, [SEC-3063], <sequence-number>, AUDIT, INFO, <system-name>, Role <role name> is copied from <source role>.`

Probable Cause Indicates a role name is copied from source role.

Recommended Action No action is required.

Severity INFO

SEC-3064

Message `<timestamp>, [SEC-3064], <sequence-number>, AUDIT, INFO, <system-name>, Permission to the RBAC class(es) <RBAC Class Names> is changed for the role <Role Name>.`

Probable Cause Indicates the permission to the RBAC class is changed for the role name.

Recommended Action No action is required.

Severity INFO

SEC-3065

Message `<timestamp>, [SEC-3065], <sequence-number>, AUDIT, INFO, <system-name>, Configuration of user-defined roles is uploaded.`

Probable Cause Indicates the configuration of user-defined roles are uploaded.

Recommended Action No action is required.

Severity INFO

SEC-3066

Message `<timestamp>, [SEC-3066], <sequence-number>, AUDIT, INFO, <system-name>, Configuration of user-defined roles is downloaded.`

Probable Cause Indicates the configuration of user-defined roles are downloaded.

Recommended Action No action is required.

Severity INFO

SEC-4001

Message `<timestamp>, [SEC-4001], <sequence-number>, AUDIT, INFO, <system-name>, Client logged in <IP Address> <User Account> <Application>.`

Probable Cause Indicates the client has logged in.

Recommended Action No action is required.

Severity INFO

Chapter

SFLOW System Messages

91

SFLO-1001

Message `<timestamp>, [SFLO-1001], <sequence-number>,, INFO, <system-name>, sFlow is <state> globally.`

Probable Cause Indicates that the sFlow is enabled or disabled globally.

Recommended Action No action is required.

Severity INFO

SFLO-1002

Message `<timestamp>, [SFLO-1002], <sequence-number>,, INFO, <system-name>, sFlow is <state> for port <name>.`

Probable Cause Indicates that the sFlow is enabled or disabled for a particular port.

Recommended Action No action is required.

Severity INFO

SFLO-1003

Message `<timestamp>, [SFLO-1003], <sequence-number>,, INFO, <system-name>, Global sFlow sampling rate is changed to <sample_rate>.`

Probable Cause Indicates that the global sampling rate has changed.

Recommended Action No action is required.

Severity INFO

SFLO-1004

Message `<timestamp>, [SFLO-1004], <sequence-number>,, INFO, <system-name>, Global sFlow polling interval is changed to <polling_intvl>.`

Probable Cause Indicates that the global counter sampling interval has changed.

Recommended Action No action is required.

Severity INFO

SFLO-1005

Message `<timestamp>, [SFLO-1005], <sequence-number>,, INFO, <system-name>, sFlow sampling rate on port <name> is changed to <sample_rate>.`

Probable Cause Indicates that the sampling rate has changed on the port.

Recommended Action No action is required.

Severity INFO

SFLO-1006

Message `<timestamp>, [SFLO-1006], <sequence-number>,, INFO, <system-name>, sFlow polling interval on port <name> is changed to <poling_intvl>.`

Probable Cause Indicates that the polling interval has changed on the port.

Recommended Action No action is required.

Severity INFO

SFLO-1007

Message `<timestamp>, [SFLO-1007], <sequence-number>,, INFO, <system-name>, <name> is as <state> as sFlow collector.`

Probable Cause Indicates that the sFlow collector is either configured or not configured.

Recommended Action No action is required.

Severity INFO

SFLO-1008

Message `<timestamp>, [SFLO-1008], <sequence-number>,, INFO, <system-name>, All the sFlow collectors are unconfigured.`

Probable Cause Indicates that all the sFlow collectors are not configured.

Recommended Action No action is required.

Severity INFO

91 SFLO-1008

Chapter

SNMP System Messages

92

SNMP-1001

Message `<timestamp>, [SNMP-1001], <sequence-number>,, ERROR, <system-name>, SNMP service is not available <Reason>.`

Probable Cause Indicates the simple network management protocol (SNMP) service could not be started because of the specified *Reason*. You will not be able to query the switch through SNMP.

Recommended Action Verify the IP address for the Ethernet and Fibre Channel interface is set correctly. If the specified *Reason* is an initialization failure, the switch has to restart.

Severity ERROR

SNMP-1002

Message `<timestamp>, [SNMP-1002], <sequence-number>,, ERROR, <system-name>, SNMP <Error Details> initialization failed.`

Probable Cause Indicates the initialization of the simple network management protocol (SNMP) service has failed and you will not be able to query the switch through SNMP.

Recommended Action Restart or power cycle the switch. This will automatically initialize SNMP.

Severity ERROR

SNMP-1003

Message `<timestamp>, [SNMP-1003], <sequence-number>,, ERROR, <system-name>, Distribution of Community Strings to Secure Fabric failed.`

Probable Cause Indicates that the changes in the simple network management protocol (SNMP) community strings could not be propagated to other switches in the secure fabric.

Recommended Action Retry changing the SNMP community strings from the primary switch.

Severity ERROR

SNMP-1004

Message `<timestamp>, [SNMP-1004], <sequence-number>, FFDC, ERROR, <system-name>, Incorrect SNMP configuration.`

Probable Cause Indicates the simple network management protocol (SNMP) configuration is incorrect and the SNMP service will not work correctly.

Recommended Action Change the SNMP configuration back to the default.

Severity ERROR

SNMP-1005

Message `<timestamp>, [SNMP-1005], <sequence-number>, AUDIT, INFO, <system-name>, SNMP configuration attribute, <Changed attribute>, has changed from <Old Value> to <New Value>`

Probable Cause Indicates the simple network management protocol (SNMP) configuration has changed. The parameter that was modified is displayed as well as the old and new values for that parameter.

Recommended Action Execute the **snmpConfig --show** command to see the new configuration.

Severity INFO

SNMP-1006

Message `<timestamp>, [SNMP-1006], <sequence-number>, AUDIT, INFO, <system-name>, <SNMP Configuration group> configuration was reset to default`

Probable Cause Indicates the simple network management protocol (SNMP) configuration group was reset to the factory default.

Recommended Action Execute the **snmpConfig --show** for the group to see the new configuration.

Severity INFO

SNMP-1007

Message `<timestamp>, [SNMP-1007], <sequence-number>,, INFO, <system-name>, The last fabric change happened at: <string>.`

Probable Cause Indicates the last fabric change time.

Recommended Action Execute the **fabricshow** command to view the current fabric status.

Severity INFO

SNMP-1008

Message `<timestamp>, [SNMP-1008], <sequence-number>,, INFO, <system-name>, The last device change happened at: <string>.`

Probable Cause Indicates the last device change time.

Recommended Action Execute the **nsshow** command to view the current device status.

Severity INFO

Chapter

SPC System Messages

93

SPC-1001

Message `<timestamp>, [SPC-1001], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, Cryptographic operation enabled.`

Probable Cause Indicates the cryptographic operation is enabled on an encryption engine.

Recommended Action No action is required.

Severity INFO

SPC-1002

Message `<timestamp>, [SPC-1002], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, Cryptographic operation disabled.`

Probable Cause Indicates the cryptographic operation is disabled on an encryption engine.

Recommended Action No action is required.

Severity INFO

SPC-1003

Message `<timestamp>, [SPC-1003], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, Security Processor faulted.`

Probable Cause Indicates the security processor is faulted because of an internal error. Cryptographic operations are affected.

Recommended Action For a bladed system, perform **slotpoweroff** and **slotpoweron** commands on the blade to recover the system. For a non-bladed system, perform a **fastboot** command on the switch to recover the system.

Severity ERROR

SPC-2001

Message `<timestamp>, [SPC-2001], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: Crypto error asserted by Vader/OB1 0x%x.`

Probable Cause Indicates the Crypto error is asserted by FPGA.

Recommended Action No action is required.

Severity ERROR

SPC-2002

Message `<timestamp>, [SPC-2002], <sequence-number>,, CRITICAL, <system-name>, <slot number containing Encryption Engine>, <module name>: Tamper Event: Crypto subsystem cover tampered.`

Probable Cause Indicates the Crypto subsystem cover is tampered.

Recommended Action EE is zeroized. User needs to run initEE and regEE.

Severity CRITICAL

SPC-2003

Message `<timestamp>, [SPC-2003], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, <module name>: Data Disable status: 0x%x.`

Probable Cause Indicates the Data disable signal status.

Recommended Action No action is required.

Severity INFO

SPC-2004

Message `<timestamp>, [SPC-2004], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: FPGA firmware download failed: 0x%x.`

Probable Cause Indicates the FPGA download has failed.

Recommended Action No action is required.

Severity ERROR

SPC-2005

Message `<timestamp>, [SPC-2005], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, <module name>: FPGA firmware download success: 0x%x.`

Probable Cause Indicates the FPGA download was successful.

Recommended Action No action is required.

Severity INFO

SPC-2006

Message `<timestamp>, [SPC-2006], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: Crypto post tests failed: 0x%x.`

Probable Cause Indicates the Crypto POST tests have failed.

Recommended Action No action is required.

Severity ERROR

SPC-2007

Message `<timestamp>, [SPC-2007], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, <module name>: Crypto post tests success: 0x%x.`

Probable Cause Indicates the Crypto POST tests passed successfully.

Recommended Action No action is required.

Severity INFO

SPC-2008

Message `<timestamp>, [SPC-2008], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, <module name>: Vader/OB1 recovered from error.`

Probable Cause Indicates the Crypto error from FPGA de-asserted.

Recommended Action No action is required.

Severity INFO

SPC-2009

Message `<timestamp>, [SPC-2009], <sequence-number>,, CRITICAL, <system-name>, <slot number containing Encryption Engine>, <module name>: Tamper event:  User zeroization.`

Probable Cause Indicates the Tamper event triggered due to a user zeroize request.

Recommended Action EE is zeroized. Run the **initEE** and **regEE** commands.

Severity CRITICAL

SPC-2010

Message `<timestamp>, [SPC-2010], <sequence-number>,, CRITICAL, <system-name>, <slot number containing Encryption Engine>, <module name>: Crypto subsystem cover is open.`

Probable Cause Indicates the Crypto subsystem cover is open.

Recommended Action Close the crypto subsystem cover properly.

Severity CRITICAL

SPC-2011

Message `<timestamp>, [SPC-2011], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, <module name>: OB1 crypto BIST success.`

Probable Cause Indicates the FPGA BIST was successful.

Recommended Action No action is required.

Severity INFO

SPC-2012

Message `<timestamp>, [SPC-2012], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, <module name>: User zeroization command completed successfully. Tamper INT status %x.`

Probable Cause Indicates the User zeroization command has completed successfully.

Recommended Action EE is zeroized. Run the **initEE** and **regEE** commands.

Severity INFO

SPC-3001

Message `<timestamp>, [SPC-3001], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: No input KEK for DEK inject, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Probable Cause Indicates the wrapping KEK for the DEK to be injected does not exist within the EE Crypto Module.

Recommended Action For opaque key vaults such as RKM, recover the missing Master Key to current or alternate position.

Severity ERROR

SPC-3002

Message `<timestamp>, [SPC-3002], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: No input KEK for DEK rewrap, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Probable Cause Indicates the input wrapping KEK for the DEK to be rewrapped does not exist within the EE Crypto Module.

Recommended Action For opaque key vaults such as RKM, recover the missing Master Key to current or alternate position.

Severity ERROR

SPC-3003

Message `<timestamp>, [SPC-3003], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: No output KEK for DEK rewrap, DEK: <DEK octet 1> <DEK octet 2> <DEK octet 3> <DEK octet 4>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Probable Cause Indicates the output wrapping KEK for the DEK to be rewrapped does not exist within the EE Crypto Module.

Recommended Action Ignore this error. The KEK will be recovered automatically.

Severity ERROR

SPC-3004

Message `<timestamp>, [SPC-3004], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: No output KEK for DEK create, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Probable Cause Indicates the output wrapping KEK for the DEK to be created does not exist within the EE Crypto Module.

Recommended Action For opaque key vaults such as RKM, recover the missing Master Key to current or alternate position.

Severity ERROR

SPC-3005

Message

```
<timestamp>, [SPC-3005], <sequence-number>,, ERROR, <system-name>, <slot number
containing Encryption Engine>, <module name>:DEK inject error: <SP status code>,
DEK: <DEK octet 1 or other info> <DEK octet 2> <DEK octet 3> <DEK octet 4>.
```

Probable Cause Indicates the cause depends on the SP status code:

- 14 - Attempt to inject a DEK to an invalid FPGA table index
- 14 - Invalid input DEK format
- 32 - DEK could not be unwrapped
- 33 - FGPA error upon inject
- 73 - Invalid KEK format

Recommended Action Contact technical support.

Severity ERROR

SPC-3006

Message

```
<timestamp>, [SPC-3006], <sequence-number>,, ERROR, <system-name>, <slot number
containing Encryption Engine>, <module name>:DEK rewrap error: <SP status code>,
DEK: <DEK octet 1 or other info> <DEK octet 2> <DEK octet 3> <DEK octet 4>.
```

Probable Cause Indicates the cause depends on the SP status code:

- 2 - Invalid input DEK format
- 14 - Rewrapping not allowed: primary KEK generation is in progress
- 31 - DEK could not be wrapped
- 32 - DEK could not be unwrapped
- 33 - FGPA error upon inject
- 73 - Invalid KEK format

Recommended Action For status code 14, complete primary KEK generation; otherwise, contact technical support.

Severity ERROR

SPC-3007

Message `<timestamp>, [SPC-3007], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: DEK create error: <SP status code>, info: <other info>.`

Probable Cause Indicates the cause depends on the SP status code:

- 2 - Invalid input DEK specification
- 21 - No primary KEK exists with which to wrap the DEK
- 14 - Creation not allowed: primary KEK generation is in progress
- 31 - DEK could not be wrapped
- 73 - Invalid KEK format
- other - Internal error

Recommended Action For status code 14, complete primary KEK generation; otherwise, contact technical support.

Severity ERROR

SPC-3008

Message `<timestamp>, [SPC-3008], <sequence-number>,, INFO, <system-name>, <slot number containing Encryption Engine>, <module name>: SP crypto got READY notification.`

Probable Cause Indicates the key application (KPD) within the Crypto Module of the EE has been started.

Recommended Action No action is required.

Severity INFO

SPC-3009

Message `<timestamp>, [SPC-3009], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: FIPS certificate mismatch, certificate: <FIPS certificate is CO-0 or User-1>.`

Probable Cause Indicates the FIPS certificate within the Crypto Module does not match that of the node.

Recommended Action Zeroize the EE (after backing up any needed primary or secondary KEK), then run initEE and regEE.

Severity ERROR

SPC-3010

Message `<timestamp>, [SPC-3010], <sequence-number>,, WARNING, <system-name>, <slot number containing Encryption Engine>, <module name>: SEK integrity failure during initialization.`

Probable Cause Indicates the Crypto Module internal Secret Encryption Key has been corrupted or has not been initialized.

Recommended Action Run the **initEE** and **regEE** commands.

Severity ERROR

SPC-3011

Message `<timestamp>, [SPC-3011], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: Persistent data storage error: <SP status code>, KEK: <KEK octet 1> <KEK octet 2> <KEK octet 3> <KEK octet 4>.`

Probable Cause Indicates an attempt to store Crypto Module internal data using the Secret Encryption Key failed - most likely, the EE has been zeroized or tampered with.

Recommended Action Run the **initEE** and **regEE** commands, then recover or restore the needed primary and secondary KEKs.

Severity ERROR

SPC-3012

Message `<timestamp>, [SPC-3012], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: Persistent data retrieval error: <SP status code>.`

Probable Cause Indicates an attempt to read Crypto Module internal data using the Secret Encryption Key failed - most likely, the EE has been zeroized or tampered with.

Recommended Action Run **initEE** and **regEE** commands, then recover or restore the needed primary and secondary KEKs.

Severity ERROR

SPC-3013

Message `<timestamp>, [SPC-3013], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: SEK generation failure: <SP status code>.`

Probable Cause Indicates the Crypto Module internal Secret Encryption Key could not be generated.

Recommended Action Contact your technical support.

Severity ERROR

SPC-3014

Message `<timestamp>, [SPC-3014], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: RNG compare failure: successive values match.`

Probable Cause Indicates the Crypto Module internal random number generator has failed.

Recommended Action Contact technical support.

Severity ERROR

SPC-3015

Message `<timestamp>, [SPC-3015], <sequence-number>,, ERROR, <system-name>, <slot number containing Encryption Engine>, <module name>: RSA pairwise key generation test failure.`

Probable Cause Indicates the Crypto Module could not generate its internal key pair.

Recommended Action Contact technical support.

Severity ERROR

93 SPC-3015

Chapter

SPM System Messages

94

SPM-1001

Message `<timestamp>, [SPM-1001], <sequence-number>,, ERROR, <system-name>, Init fails: <Reason>.`

Probable Cause Indicates the SPM has failed to initialize.

Recommended Action Check the system resources and restart the switch.

Severity ERROR

SPM-1002

Message `<timestamp>, [SPM-1002], <sequence-number>,, WARNING, <system-name>, Generic SPM Warning: <Reason>.`

Probable Cause Indiactes an SPM warning based on the reason displayed.

Recommended Action Run the **supportsave** command to gather information.

Severity WARNING

SPM-1003

Message `<timestamp>, [SPM-1003], <sequence-number>,, INFO, <system-name>, Set New Group Cfg SC Enable <SC_Enable> KV Type <KV_Type>.`

Probable Cause Indicates a new group has been configured.

Recommended Action No action is required.

Severity INFO

SPM-1004

Message `<timestamp>, [SPM-1004], <sequence-number>,, INFO, <system-name>, Initialize Node.`

Probable Cause Indicates a node initialization.

Recommended Action No action is required.

Severity INFO

SPM-1005

Message `<timestamp>, [SPM-1005], <sequence-number>,, INFO, <system-name>, Set EE Control slot <slot> action <action>.`

Probable Cause Indicates encryption engine (EE) control slot configuration.

Recommended Action No action is required.

Severity INFO

SPM-1006

Message `<timestamp>, [SPM-1006], <sequence-number>,, INFO, <system-name>, Registered Certificate of type <cert_type>.`

Probable Cause Indicates a certificate registration.

Recommended Action No action is required.

Severity INFO

SPM-1007

Message `<timestamp>, [SPM-1007], <sequence-number>,, INFO, <system-name>, Deregistered Certificate cid [<cert_id>] type <cert_type> idx <qc_idx>.`

Probable Cause Indicates a certificate de-registration.

Recommended Action No action is required.

Severity INFO

SPM-1008

Message `<timestamp>, [SPM-1008], <sequence-number>,, INFO, <system-name>, Deregistered SP Certificate in slot <slot>.`

Probable Cause Indicates an SP certificate de-registration.

Recommended Action No action is required.

Severity INFO

SPM-1009

Message `<timestamp>, [SPM-1009], <sequence-number>,, ERROR, <system-name>, <cert> Certificate is missing.`

Probable Cause Indicates that a certificate is missing.

Recommended Action Run the **cryptocfg –initnode** command.

Severity ERROR

SPM-1010

Message `<timestamp>, [SPM-1010], <sequence-number>,, ERROR, <system-name>, <cert> Key Vault Certificate is missing.`

Probable Cause Indicates that a key vault certificate is missing.

Recommended Action Deregister and register this key vault.

Severity ERROR

SPM-1011

Message `<timestamp>, [SPM-1011], <sequence-number>,, INFO, <system-name>, Group Cfg Changed Quorum Size <qc_size>.`

Probable Cause Indicates that a group configuration has changed the quorum size.

Recommended Action No action is required.

Severity INFO

SPM-1012

Message `<timestamp>, [SPM-1012], <sequence-number>,, INFO, <system-name>, Authentication Context:<established>.`

Probable Cause Indicates an authentication context.

Recommended Action No action is required.

Severity INFO

SPM-1013

Message `<timestamp>, [SPM-1013], <sequence-number>,, ERROR, <system-name>, Security database is out of sync.`

Probable Cause Indicates a failure to distribute security database.

Recommended Action Use **cryptocfg –sync -securitydb** to manually sync security db.

Severity ERROR

SPM-1014

Message `<timestamp>, [SPM-1014], <sequence-number>,, WARNING, <system-name>, Warning: Configdownload results in EE going to Operational; Need valid KEK state.`

Probable Cause Indicates the Master Keys downloaded will not be effective unless imported as the EE may have different MK configured.

Recommended Action Import required MK(s) using **cryptocfg –recovermastekey** command to bring EE online.

Severity WARNING

SPM-1015

Message `<timestamp>, [SPM-1015], <sequence-number>,, WARNING, <system-name>, Security database may be out of sync.`

Probable Cause Indicates a failure to distribute security database.

Recommended Action Use **cryptocfg –sync -securitydb** to manually sync security db.

Severity WARNING

SPM-3001

Message `<timestamp>, [SPM-3001], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: Node <wwnstr> initialized.`

Probable Cause Indicates a node was initialized.

Recommended Action No action is required.

Severity INFO

SPM-3002

Message `<timestamp>, [SPM-3002], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: EE in slot <slot> initialized.`

Probable Cause Indicates an encryption engine was initialized.

Recommended Action No action is required.

Severity INFO

SPM-3003

Message `<timestamp>, [SPM-3003], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: EE in slot <slot> registered.`

Probable Cause Indicates an encryption engine was registered.

Recommended Action No action is required.

Severity INFO

SPM-3004

Message `<timestamp>, [SPM-3004], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: EE in slot <slot> enabled.`

Probable Cause Indicates an encryption engine was enabled.

Recommended Action No action is required.

Severity INFO

SPM-3005

Message `<timestamp>, [SPM-3005], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: EE in slot <slot> disabled.`

Probable Cause Indicates an encryption engine was disabled.

Recommended Action No action is required.

Severity INFO

SPM-3006

Message
```
<timestamp>, [SPM-3006], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: <source file> file exported via scp: <hostUsername>
[<hostIP>]:<hostPath>.
```

Probable Cause Indicates a file was exported using SCP protocol.

Recommended Action No action is required.

Severity INFO

SPM-3007

Message
```
<timestamp>, [SPM-3007], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: <source file> file imported via scp: <hostUsername>
[<hostIP>]:<hostPath>.
```

Probable Cause Indicates a file was imported using SCP protocol.

Recommended Action No action is required.

Severity INFO

SPM-3008

Message
```
<timestamp>, [SPM-3008], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: DH challenge generated for vault IP <vaultIP>.
```

Probable Cause Indicates a DH challenge was generated for a key vault.

Recommended Action No action is required.

Severity INFO

SPM-3009

Message
```
<timestamp>, [SPM-3009], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: DH response accepted.
```

Probable Cause Indicates a DH challenge was accepted.

Recommended Action No action is required.

Severity INFO

SPM-3010

Message `<timestamp>, [SPM-3010], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: EE in slot <slot> zeroized.`

Probable Cause Indicates an encryption engine was zeroized.

Recommended Action No action is required.

Severity INFO

SPM-3011

Message `<timestamp>, [SPM-3011], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: Local file \"<filename>\" deleted.`

Probable Cause Indicates a locally stored file was deleted.

Recommended Action No action is required.

Severity INFO

SPM-3012

Message `<timestamp>, [SPM-3012], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: <primaryOrSecondary> key vault registered.  Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\" IP address: <IPAddress>.`

Probable Cause Indicates a key vault was registered.

Recommended Action No action is required.

Severity INFO

SPM-3013

Message `<timestamp>, [SPM-3013], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: Key vault with certificate label \"<certLabel>\" deregistered.`

Probable Cause Indicates a key vault was de-registered.

Recommended Action No action is required.

Severity INFO

SPM-3014

Message
```
<timestamp>, [SPM-3014], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: Key archive client registered with certificate file
\"<certFilename>\".
```

Probable Cause Indicates a KAC certificate was registered.

Recommended Action No action is required.

Severity INFO

SPM-3015

Message
```
<timestamp>, [SPM-3015], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: Key vault type set to <keyVaultType>.
```

Probable Cause Indicates the key vault type was set.

Recommended Action No action is required.

Severity INFO

SPM-3016

Message
```
<timestamp>, [SPM-3016], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: Master key generated.
```

Probable Cause Indicates a master key was generated.

Recommended Action No action is required.

Severity INFO

SPM-3017

Message
```
<timestamp>, [SPM-3017], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: Master key exported.
```

Probable Cause Indicates a master key was exported.

Recommended Action No action is required.

Severity INFO

SPM-3018

Message `<timestamp>, [SPM-3018], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: <currentOrAlternate>master key recovered.`

Probable Cause Indicates a master key was recovered.

Recommended Action No action is required.

Severity INFO

SPM-3019

Message `<timestamp>, [SPM-3019], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: System card registered.  Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Probable Cause Indicates a system card was registered.

Recommended Action No action is required.

Severity INFO

SPM-3020

Message `<timestamp>, [SPM-3020], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: System card with certificate label \"<certLabel>\" deregistered.`

Probable Cause Indicates a system card was de-registered.

Recommended Action No action is required.

Severity INFO

SPM-3021

Message `<timestamp>, [SPM-3021], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: Authentication card registered.  Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Probable Cause Indicates an authentication card was registered.

Recommended Action No action is required.

Severity INFO

SPM-3022

Message
```
<timestamp>, [SPM-3022], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: Authentication card with certificate label \"<certLabel>\"
deregistered.
```

Probable Cause Indicates an authentication card was de-registered.

Recommended Action No action is required.

Severity INFO

SPM-3023

Message
```
<timestamp>, [SPM-3023], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: System card <enabledOrDisabled>.
```

Probable Cause Indicates use of the system card was enabled or disabled.

Recommended Action No action is required.

Severity INFO

SPM-3024

Message
```
<timestamp>, [SPM-3024], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: Quorum size set to <quorumsize>.
```

Probable Cause Indicates the quorum size was set.

Recommended Action No action is required.

Severity INFO

SPM-3025

Message
```
<timestamp>, [SPM-3025], <sequence-number>,, INFO, <system-name>,Event: cryptocfg
Status: success, Info: File imported via usb: Source: <sourcePath> Destination:
<destinationFilename>.
```

Probable Cause Indicates a file was imported through the USB device.

Recommended Action No action is required.

Severity INFO

SPM-3026

Message `<timestamp>, [SPM-3026], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: File exported via usb: Source: <sourcePath> Destination: <destinationFilename>.`

Probable Cause Indicates a file was exported through the USB device.

Recommended Action No action is required.

Severity INFO

SPM-3027

Message `<timestamp>, [SPM-3027], <sequence-number>,, INFO, <system-name>,Event: cryptocfg Status: success, Info: Recovery card registered.  Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Probable Cause Indicates a recovery card was registered.

Recommended Action No action is required.

Severity INFO

SPM-3028

Message `<timestamp>, [SPM-3028], <sequence-number>,, INFO, <system-name>, Event: SPM-EE state changed, Info: EE State: <EE Status>.`

Probable Cause Indicates an EE state has changed.

Recommended Action No action is required.

Severity INFO

SPM-3029

Message `<timestamp>, [SPM-3029], <sequence-number>,, INFO, <system-name>, Event: KeyVault Connection Status: <status>, Info:KAC_Connect: <kac status>.`

Probable Cause Indicates the status of key vault.

94 SPM-3029

Recommended Action No action is required.

Severity INFO

Chapter

SS System Messages

95

SS-1000

Message `<timestamp>, [SS-1000], <sequence-number>,, INFO, <system-name>, supportSave has uploaded support information to the host with IP address <host ip>.`

Probable Cause Indicates the **supportSave** command was used to transfer support information to a remote location.

Recommended Action No action is required.

Severity INFO

SS-1001

Message `<timestamp>, [SS-1001], <sequence-number>,, WARNING, <system-name>, supportSave's upload operation to host IP address <host ip> aborted.`

Probable Cause Indicates a file copy error has occurred during execution of the **supportSave** command. Complete error information cannot always be displayed in this message due to possible errors in subcommands being executed by the **supportSave** command.

Recommended Action Check the remote server settings. Run the **supportFtp** command to set the FTP or SCP parameters. After the problem is corrected, rerun the **supportSave** command.

Severity WARNING

SS-1002

Message `<timestamp>, [SS-1002], <sequence-number>,, INFO, <system-name>, supportSave has stored support information to the USB storage device.`

Probable Cause Indicates the **supportSave** command was used to transfer support information to an attached USB storage device.

Recommended Action No action is required.

Severity INFO

SS-1003

Message `<timestamp>, [SS-1003], <sequence-number>,, WARNING, <system-name>, supportSave's operation to USB storage device aborted.`

Probable Cause Indicates a USB operation error has occurred during execution of the **supportSave** command. Complete error information cannot always be displayed in this message due to possible errors in subcommands being executed by the **supportSave** command.

Recommended Action Run the **usbstorage** command to check the USB storage device settings. After the USB problem is corrected, rerun the **supportSave** command.

Severity WARNING

SS-1004

Message `<timestamp>, [SS-1004], <sequence-number>,, WARNING, <system-name>, One or more modules timed out during supportsave. Please retry supportsave with -t option to collect all logs.`

Probable Cause Indicates timeout in modules during supportsave.

Recommended Action Run **supportsave -t [2-5]** to collect all logs.

Severity WARNING

SS-1005

Message `<timestamp>, [SS-1005], <sequence-number>,, WARNING, <system-name>, supportsave failed for the slot <Slot Number>. Reason: No IP connection.`

Probable Cause Indicates the IP connection between Active CP and the blade in the corresponding slot does not exist.

Recommended Action Check for the IP connection between Active CP and the corresponding slot. Once the IP connection gets established rerun the **supportsave** command.

Severity WARNING

SS-1006

Message `<timestamp>, [SS-1006], <sequence-number>,, WARNING, <system-name>, supportsave failed for the slot <Slot Number>. Reason: supportsave request was not sent to the blade in the corresponding slot.`

Probable Cause Indicates the supportsave request was not sent to the blade in the corresponding slot.

Recommended Action Reboot the switch and then run the **supportsave** command.

Severity WARNING

SS-1007

Message `<timestamp>, [SS-1007], <sequence-number>,, WARNING, <system-name>, supportsave failed for the slot <Slot Number>. Reason: No response from the blade in the corresponding slot for the given ss request.`

Probable Cause Indicates no reponse from the blade in the corresponding slot for the given supportsave request.

Recommended Action Reboot the switch and then run the **supportsave** command.

Severity WARNING

SS-1008

Message `<timestamp>, [SS-1008], <sequence-number>,, WARNING, <system-name>, supportsave failed for the slot <Slot Number>. Reason: BP supportsave timeout.`

Probable Cause Indicates that the corresponding slot has taken more time than expected, to collect the supportsave logs.

Recommended Action Rerun the **supportsave** command.

Severity WARNING

95 SS-1008

Chapter

SSM System Messages

96

SSMD-1001

Message `<timestamp>, [SSMD-1001], <sequence-number>,, ERROR, <system-name>,Failed to allocate memory: <function name>.`

Probable Cause Indicates that the specified function has failed to allocate memory.

Recommended Action Check the memory usage on the switch using the **memShow** command.

Restart or power cycle the switch.

Severity ERROR

SSMD-1002

Message `<timestamp>, [SSMD-1002], <sequence-number>,, ERROR, <system-name>,Failed to initialize <module> rc = <error>.`

Probable Cause Indicates that an initialization of a module within the SSM has failed.

Recommended Action Download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

SSMD-1003

Message `<timestamp>, [SSMD-1003], <sequence-number>,, ERROR, <system-name>,Failed to lock semaphore mutex: <function name>.`

Probable Cause Indicates that the specified function has failed to lock the mutex (semaphore).

Recommended Action Restart or power cycle the switch.

Severity ERROR

SSMD-1004

Message `<timestamp>, [SSMD-1004], <sequence-number>,, ERROR, <system-name>,Failed to unlock semaphore mutex: <function name>.`

Probable Cause Indicates that the specified function has failed to unlock the mutex (semaphore).

Recommended Action Restart or power cycle the switch.

Severity ERROR

SSMD-1005

Message `<timestamp>, [SSMD-1005], <sequence-number>,, ERROR, <system-name>,SSM startup failed.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected, severe error during basic startup and initialization.

Recommended Action Restart or power cycle the switch .If the condition persists then download a new firmware version using the **firmwareDownload** command. Refer to the *Fabric OS Command Reference Manual* for more information on this command.

Severity ERROR

SSMD-1200

Message `<timestamp>, [SSMD-1200], <sequence-number>,, WARNING, <system-name>,QoS failed programming ASIC <ASIC slot number> / <ASIC chip number>.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for the enforcing Multicast Rate Limit feature.

Recommended Action Delete and reapply QoS Multicast Rate Limit policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1201

Message `<timestamp>, [SSMD-1201], <sequence-number>,, WARNING, <system-name>,QoS failed programming ASIC <ASIC slot number> / <ASIC chip number> Multicast Tail Drop.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for the enforcing Multicast Tail Drop feature.

Recommended Action Delete and reapply QoS Multicast Tail Drop policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1202

Message `<timestamp>, [SSMD-1202], <sequence-number>,, WARNING, <system-name>,QoS failed programming interface 0x<Interface ID> x 802.3x Pause flow control.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the interface 802.3x Pause flow control feature.

Recommended Action Delete and reapply QoS 802.3x Pause flow control policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1203

Message `<timestamp>, [SSMD-1203], <sequence-number>,, WARNING, <system-name>,QoS failed programming interface 0x <Interface ID> x PFC flow control.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the interface PFC flow control feature.

Recommended Action Delete and reapply QoS 802.3x Pause flow control policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1204

Message `<timestamp>, [SSMD-1204], <sequence-number>,, WARNING, <system-name>,QoS failed initializing ASIC <ASIC slot number> / <ASIC chip number>.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in initializing the dataplane ASIC QoS infrastructure.

Recommended Action Restart or power cycle the switch.

Severity WARNING

SSMD-1205

Message `<timestamp>, [SSMD-1205], <sequence-number>,, WARNING, <system-name>,CEE failed programming ETS policy for CEE Map <CEE Map name>.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the CEE Map ETS feature.

Recommended Action Delete and reapply the CEE Map ETS policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1206

Message `<timestamp>, [SSMD-1206], <sequence-number>,, WARNING, <system-name>,CEE failed programming CoS to PGID policy for CEE Map <CEE Map name>.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the CEE Map CoS to PGID mapping feature.

Recommended Action Delete and reapply the CEE Map CoS to PGID policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1207

Message `<timestamp>, [SSMD-1207], <sequence-number>,, WARNING, <system-name>,QoS failed programming interface 0x <Interface ID> x Default CoS.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the interface Default CoS feature.

Recommended Action Delete and reapply the QoS interface Default CoS policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1208

Message `<timestamp>, [SSMD-1208], <sequence-number>,, WARNING, <system-name>,QoS failed programming interface 0x <Interface ID> x Trust.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the interface Trust feature.

Recommended Action Delete and reapply the QoS interface Trust policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1209

Message `<timestamp>, [SSMD-1209], <sequence-number>,, WARNING, <system-name>,QoS failed programming interface 0x <Interface ID> x CoS Mutation map.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the iCoS Mutation mapping feature.

Recommended Action Delete and reapply the QoS interface CoS Mutation policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1210

Message `<timestamp>, [SSMD-1210], <sequence-number>,, WARNING, <system-name>,QoS failed programming interface 0x <Interface ID> x CoS to Traffic Class map.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the CoS to Traffic Class mapping feature.

Recommended Action Delete and reapply the QoS interface CoS to Traffic Class policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1211

Message `<timestamp>, [SSMD-1211], <sequence-number>,, WARNING, <system-name>,QoS failed programming ASIC <ASIC slot number> / <ASIC chip number> Scheduler Control.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the packet Scheduler Control feature.

Recommended Action Delete and reapply the QoS packet Scheduler Control policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1212

Message `<timestamp>, [SSMD-1212], <sequence-number>,, WARNING, <system-name>,QoS failed programming ASIC <ASIC slot number> / <ASIC chip number> Multicast Scheduler Control.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the multicast packet Scheduler Control feature.

Recommended Action Delete and reapply the QoS packet Scheduler Control policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1213

Message `<timestamp>, [SSMD-1213], <sequence-number>,, WARNING, <system-name>,QoS failed programming interface 0x <Interface ID> x CoS Tail Drop Threshold.`

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the interface CoS Tail Drop Threshold feature.

Recommended Action Delete and reapply the QoS CoS Tail Drop Threshold policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1214

Message

```
<timestamp>, [SSMD-1214], <sequence-number>,, WARNING, <system-name>,QoS failed
programming interface 0x <Interface ID> x CoS Tail Drop Threshold.
```

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the interface CoS Tail Drop Threshold feature.

Recommended Action Delete and reapply the QoS CoS Tail Drop Threshold policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1215

Message

```
<timestamp>, [SSMD-1215], <sequence-number>,, WARNING, <system-name>,QoS failed
programming interface 0x <Interface ID> x CoS Tail Drop Threshold.
```

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the interface CoS Tail Drop Threshold feature.

Recommended Action Delete and reapply the QoS CoS Tail Drop Threshold policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1216

Message

```
<timestamp>, [SSMD-1216], <sequence-number>,, WARNING, <system-name>,QoS failed
programming interface 0x <Interface ID> x Pause.
```

Probable Cause Indicates the DCE System Services Manager (SSM) encountered an unexpected error in programming the dataplane ASIC for enforcing the interface Pause feature.

Recommended Action Delete and reapply the QoS Pause policy. Restart or power cycle the switch.

Severity WARNING

SSMD-1217

Message `<timestamp>, [SSMD-1217], <sequence-number>,, WARNING, <system-name>,QoS CEE could not comply with FCoE scheduler policy for CEE Map <CEE Map name>.`

Probable Cause Indicates the DCE System Services Manager (SSM) was unable to translate CEE Map and FCoE configuration into an ETS scheduler policy implementable by the dataplane ASIC.

Recommended Action Redefine CEE Map and FCoE into a configuration that translates into into an ETS scheduler policy requiring 8 or fewer Traffic Class.

Severity WARNING

SSMD-1300

Message `<timestamp>, [SSMD-1300], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> is created with precedence <precedence>.`

Probable Cause Indicates that a CEEMap is created.

Recommended Action No action is required.

Severity INFO

SSMD-1301

Message `<timestamp>, [SSMD-1301], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> is deleted.`

Probable Cause Indicates that a CEEMap is deleted.

Recommended Action No action is required.

Severity INFO

SSMD-1302

Message `<timestamp>, [SSMD-1302], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> priority table <pg_ids> is <action>.`

Probable Cause Indicates that PGs added to or removed from existing ceemap.

Recommended Action No action is required.

Severity INFO

SSMD-1303

Message `<timestamp>, [SSMD-1303], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> priority group <pg_id> with weight <PGID_weight> is created with pfc <pfc>.`

Probable Cause Indicates that priority Group has been created.

Recommended Action No action is required.

Severity INFO

SSMD-1304

Message `<timestamp>, [SSMD-1304], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> priority group <pg_id> is deleted.`

Probable Cause Indicates that priority Group has been deleted.

Recommended Action No action is required.

Severity INFO

SSMD-1305

Message `<timestamp>, [SSMD-1305], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> priority group <pg_id> weight is changed from <PGID_weight_new> to <PGID_weight_old>.`

Probable Cause Indicates that priority Group weight has been changed.

Recommended Action No action is required.

Severity INFO

SSMD-1306

Message `<timestamp>, [SSMD-1306], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> priority group <pg_id> is PFC <pfc_status>.`

Probable Cause Indicates that priority Group pfc status has been changed.

Recommended Action No action is required.

Severity INFO

SSMD-1307

Message `<timestamp>, [SSMD-1307], <sequence-number>,, INFO, <system-name>, <acl_type> access list <acl_name> is created.`

Probable Cause Indicates that Access List has been created.

Recommended Action No action is required.

Severity INFO

SSMD-1308

Message `<timestamp>, [SSMD-1308], <sequence-number>,, INFO, <system-name>, <acl_type> access list <acl_name> is deleted.`

Probable Cause Indicates that Access List has been deleted.

Recommended Action No action is required.

Severity INFO

SSMD-1309

Message `<timestamp>, [SSMD-1309], <sequence-number>,, INFO, <system-name>, <acl_type> access list <acl_name> rule sequence number <rule_sq_no> is <action>.`

Probable Cause Indicates that Access List rules added to or removed from existing policy.

Recommended Action No action is required.

Severity INFO

SSMD-1310

Message `<timestamp>, [SSMD-1310], <sequence-number>,, INFO, <system-name>, ACL <acl_name> configured on interface <InterfaceName>.`

Probable Cause Indicates that Access List has been configured on an interface.

Recommended Action No action is required.

Severity INFO

SSMD-1311

Message `<timestamp>, [SSMD-1311], <sequence-number>,, INFO, <system-name>, ACL <acl_name> is removed from interface <InterfaceName>.`

Probable Cause Indicates that Access List has been removed from an interface.

Recommended Action No action is required.

Severity INFO

SSMD-1312

Message `<timestamp>, [SSMD-1312], <sequence-number>,, INFO, <system-name>, <map_type> <map_name> assigned to interface <InterfaceName>.`

Probable Cause Indicates that user profile Map is assigned to an interface.

Recommended Action No action is required.

Severity INFO

SSMD-1313

Message `<timestamp>, [SSMD-1313], <sequence-number>,, INFO, <system-name>, <map_type> <map_name> removed from interface <InterfaceName>.`

Probable Cause Indicates that user profile Map is removed from interface.

Recommended Action No action is required.

Severity INFO

SSMD-1314

Message `<timestamp>, [SSMD-1314], <sequence-number>,, INFO, <system-name>, CEEMap <ceemap> precedence changed from <precedence_old> to <precedence_new>.`

Probable Cause Indicates that CEEMap precedence has been changed.

Recommended Action No action is required.

Severity INFO

Chapter

SULB System Messages

97

SULB-1001

Message `<timestamp>, [SULB-1001], <sequence-number>, AUDIT, WARNING, <system-name>, Firmwaredownload command has started.`

Probable Cause Indicates the **firmwareDownload** command has been started. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended Action Do not fail over or power down the system during firmware upgrade. Allow the **firmwareDownload** command to continue without disruption.

Run the **firmwareDownloadStatus** command for more information.

Severity WARNING

SULB-1002

Message `<timestamp>, [SULB-1002],<sequence-number>, AUDIT, INFO, <system-name>, Firmwaredownload command has completed successfully.`

Probable Cause Indicates the **firmwareDownload** command has completed successfully and switch firmware has been updated.

Recommended Action No action is required. The **firmwareDownload** command has completed as expected.

Run the **firmwareDownloadStatus** command for more information. Run the **firmwareShow** command to verify the firmware versions.

Severity INFO

SULB-1003

Message `<timestamp>, [SULB-1003], <sequence-number>, AUDIT, INFO, <system-name>, Firmwarecommit has started.`

Probable Cause Indicates that the **firmwareCommit** command has been started.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1004

Message `<timestamp>, [SULB-1004], INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwarecommit has completed.`

Probable Cause Indicates the **FirmwareCommit** command is executed.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1005

Message `<timestamp>, [SULB-1005], <sequence-number>,, INFO, <system-name>, Current Active CP is preparing to failover.`

Probable Cause Indicates the active CP is about to restart. The standby CP is taking over as the active CP.

Recommended Action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1006

Message `<timestamp>, [SULB-1006], <sequence-number>,, INFO, <system-name>, Forced failover succeeded. New Active CP is running new firmware.`

Probable Cause Indicates the previous standby CP has now become the active CP and is running the new firmware version.

Recommended Action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1007

Message `<timestamp>, [SULB-1007], <sequence-number>,, INFO, <system-name>, Standby CP reboots.`

Probable Cause Indicates the standby CP is rebooting with new firmware.

Recommended Action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1008

Message `<timestamp>, [SULB-1008], <sequence-number>,, INFO, <system-name>, Standby CP booted successfully with new firmware.`

Probable Cause Indicates the standby CP has rebooted successfully.

Recommended Action No action is required. The **firmwareDownload** command is progressing as expected.

Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1009

Message `AUDIT, <timestamp>, [SULB-1009], AUDIT, INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwaredownload command failed. status: 0x<status code>, error: 0x<error code>.`

Probable Cause Indicates the **firmwareDownload** command failed. The additional *status code* and *error code* provide debugging information.

Table lists **firmwareDownload** status messages and status codes. Some of them will not show up in this RASLOG message.

TABLE 6 Status Messages and Status Codes

Status Message	Status Code
“**firmwareDownload** sanity check failed.”	0x30
"Sanity check failed because system is non-redundant."	0x31
“Sanity check failed because **firmwareDownload** is already in progress.”	0x32
"Sanity check failed because FABRIC OS is disabled on Active CP."	0x33
"Sanity check failed because HAMD is disabled on Active CP."	0x34
“Sanity check failed because **firmwareDownload** is already in progress.”	0x35
"Sanity check failed because FABRIC OS is disabled on Standby CP."	0x36
"Sanity check failed because HAMD is disabled on Standby CP."	0x37
“**firmwareDownload** failed on Standby CP.”	0x40
“**firmwareDownload** failed on Standby CP.”	0x41
“**firmwareDownload** failed on Standby CP.”	0x42
“**firmwareCommit** failed on Standby CP.”	0x43
“**firmwareDownload** failed.”	0x44
“**firmwareDownload** failed due to IPC error.”	0x50
"Unable to check the firmware version on Standby CP due to IPC error."	0x51
“**firmwareDownload** failed due to IPC error.”	0x52
“**firmwareDownload** failed due to IPC error.”	0x53
"Standby CP failed to reboot due to IPC error."	0x54

TABLE 6 Status Messages and Status Codes

Status Message	Status Code
“**firmwareCommit** operation failed due to IPC error.”	0x55
"Unable to check the firmware version on Standby CP due to IPC error."	0x56
“Unable to restore the original firmware due to Standby CP timeout.”	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check the firmware version on Standby CP due to IPC error."	0x59
“Sanity check failed because **firmwareDownload** is already in progress.”	0x60
“Sanity check failed because **firmwareDownload** is already in progress.”	0x61
NOT USED	0x62
"System Error."	0x63
"Active CP forced failover succeeded. Now this CP becomes Active."	0x64
"Standby CP booted up."	0x65
"Active and Standby CP failed to gain HA synchronization within 10 minutes."	0x66
"Standby rebooted successfully."	0x67
"Standby failed to reboot."	0x68
“**firmwareCommit** has started to restore the secondary partition.”	0x69
"Local CP is restoring its secondary partition."	0x6a
“Unable to restore the secondary partition. Please use **firmwareDownloadStatus** and **firmwareShow** to see firmware status.”	0x6b
“**firmwareDownload** has started on Standby CP. It might take up to 10 minutes.”	0x6c
“**firmwareDownload** has completed successfully on Standby CP.”	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
“**firmwareDownload** has completed successfully on Standby CP.”	0x72
“**firmwareDownload** has started on Standby CP. It might take up to 10 minutes.”	0x73
“**firmwareDownload** has completed successfully on Standby CP.”	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76
“**firmwareCommit** has started on Standby CP.”	0x77
“**firmwareCommit** has completed successfully on Standby CP.”	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
“**firmwareCommit** has started on both Active and Standby CPs.”	0x7b
“**firmwareCommit** has completed successfully on both CPs.”	0x7c
“**firmwareCommit** failed on Active CP.”	0x7d

TABLE 6 Status Messages and Status Codes

Status Message	Status Code
"The original firmware has been restored successfully on Standby CP."	0x7e
"Unable to restore the original firmware on Standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
"There was an unexpected reboot during **firmwareDownload**. The command is aborted."	0x84
"Standby CP was not responding. The command is aborted."	0x85
"**firmwareCommit** has started on both CPs. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status."	0x86
"**firmwareCommit** has started on the local CP. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status."	0x87
"**firmwareCommit** has started on the remote CP. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status."	0x88
"Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status."	0x89
"**firmwareDownload** command has completed successfully."	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e
"**firmwareDownload** has started."	0x8f
"**firmwareCommit** has started."	0x90
"**firmwareDownload** has completed successfully."	0x91
"**firmwareCommit** has completed successfully."	0x92
"**firmwareCommit** has started to restore the secondary partition."	0x93
"**firmwareCommit** failed."	0x94
"The secondary partition has been restored successfully."	0x95
"Firmware is being downloaded to the blade. This step may take up to 10 minutes."	0xa0
"**firmwareDownload** timed out."	0xa1
"Reboot occurred during **firmwareDownload**. **firmwareCommit** will be started to recover the blade."	0xa2
"Blade rebooted during **firmwareCommit**. The operation will be restarted."	0xa3
"Firmware has been downloaded successfully. Blade is rebooting with the new firmware."	0xa4
"Blade has rebooted successfully."	0xa5
"New firmware failed to boot up. Please retry **firmwareDownload**."	0xa6
"**firmwareCommit** has started on the blade. This may take up to 10 minutes."	0xa7

TABLE 6 Status Messages and Status Codes

Status Message	Status Code
“**firmwareRestore** is entered. System will reboot and a **firmwareCommit** operation will start upon boot up.”	0xa8
"Switch is relocating the AP image."	0xa9
"The AP image is relocated successfully."	0xaa
"Switch reboots during relocating the AP image. The operation will be restarted."	0xab
“Blade failed to reboot with the original image. **firmwareRestore** command failed.”	0xac

Table 7 lists additional **firmwareDownload** error messages and error codes. They provide more details on why **firmwareDownload** failed.

TABLE 7 Error Messages and Error Codes

Error Message	Error Code
"Image is up-to-date. No need to download the same version of firmware."	0xF
“Upgrade is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding.”	0x10
“OSRootPartition is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding. For example: swap OSRootPartitions and reboot.”	0x11
“Unable to access the required package list file. Check whether the switch is supported by the requested firmware. Also check **firmwareDownload** help page for other possible failure reasons.”	0x12
"The RPM package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
“Error in getting lock device for **firmwareDownload**.”	0x18
“Error in releasing lock device for **firmwareDownload**.”	0x19
“**firmwareCommit** failed.”	0x1a
"Firmware directory structure is not compatible. Check whether the firmware is supported on this platform."	0x1b
"Failed to load the Linux kernel image."	0x1c
“OSLoader is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding.”	0x1d
“New image has not been committed. Run **firmwareCommit** or **firmwareRestore** first and then try **firmwareDownload**.”	0x1e
“**firmwareRestore** failed.”	0x1f
"Both images are mounted to the same device."	0x20
“Unable to unionist old packages.”	0x21
“**firmwareDownload** is already in progress.”	0x22

TABLE 7 Error Messages and Error Codes

Error Message	Error Code
“**firmwareDownload** timed out.”	0x23
"Our of disk space."	0x24
“Primary filesystem is inconsistent. Run **firmwareRestore** to restore the original firmware, or contact your service provider for recovery.”	0x25
"The post-install script failed."	0x26
"Unexpected reboot."	0x27
"Primary kernel partition is inconsistent. Please contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
“The platform option is not supported. Run **chassisConfig** to reset the option first and then try **firmwareDownload**.”	0x2a
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version first and then download the desired version."	0x2c
“Cannot download 5.1 because Device Based Routing policy is not supported by 5.1. Use **aptPolicy** to change the routing policy before proceeding.”	0x2d
"Invalid RPM package. Please reload firmware packages on the file server."	0x2e
"Cannot downgrade due to presence of blade type 17. Remove or power off these blades before proceeding."	0x2f
"Cannot downgrade due to presence of blade type 24. Remove or power off these blades before "	0x30
"Cannot downgrade due to presence of long-distance ports in LS mode. Please remove these settings before proceeding."	0x31
"Network is not reachable. Please verify the IP address of the server is correct."	0x32

The following section explains the causes of some common error messages:

0x15 - Failed to download Red Hat package manager (RPM) package. If this error occurs immediately after **firmwareDownload** is started, the firmware on the switch may be two releases older than the requested firmware. **firmwareDownload** supports firmware upgrades within two feature releases (a feature release is indicated by a major number and a minor number, for example, X.Y). The following are major upgrade versions for the Fabric OS: v4.0, v4.1, v4.2, v4.4, v5.0, v5.1.,5.2, and 5.3. In this case, you will need to upgrade to an intermediate version before downloading the desired version. If this error occurs in the middle of **firmwareDownload**, the firmware in the file server may be corrupted or there may be a temporary network issue. In this case, retry the **firmwareDownload** command. If the problem persists, contact your system administrator.

0x18 - Error in getting lock device for **firmwareDownload**. This error may occur because another **firmwareDownload** is already in progress. Run **firmwareDownloadStatus** to verify that this is the case. Wait for the current session to finish before proceeding.

0x23 - **firmwareDownload** timed out. This error may occur because **firmwareDownload** has not completed within the predefined timeout period. It is most often caused by network issues. If the problem persists, contact your system administrator.

0x24 - out of disk space. This error may occur because some coredump files have not been removed from the filesystem and are using up disk space. Remove these coredump files using the **supportSave** command before proceeding.

0x29 - The pre-install script failed. This error may be caused by an unsupported blade type in the chassis. Remove or power off the unsupported blades before proceeding. Another possible cause may be an invalid **chassisConfig** option setting. In that case, reset the **chassisConfig** option before retrying **firmwareDownload**.

0x2e - Invalid Red Hat package manager (RPM) package. This error maybe caused by an inconsistent firmware image loaded on the file server. It may also be caused by temporary networking issues. Please reload firmware packages on the file server, then retry **firmwareDownload**. If the problem persists, contact your system administrator.

Table 8 lists the **firmwareDownload** state names and state values. They indicate where in the **firmwareDownload** process the error occurred.

TABLE 8 Upgrade State and Code Value

Upgrade State	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

Recommended Action

Run the **firmwareDownloadStatus** command for more information.

In a director-class switch, when **firmwareDownload** fails, the command will synchronize the firmware on the two partitions of each CP by starting a firmware commit operation. Wait until this operation completes (about 10 minutes) before attempting another **firmwareDownload**.

In a director-class switch, when **firmwareDownload** fails, the two CPs may end up with different versions of firmware and they may not gain high-availability (HA) sync. In that case, run **firmwareDownload** single mode (**-s**) to upgrade the firmware on the standby CP to the same version as the active CP. Then retry **firmwareDownload** to download the desired version of firmware onto the CPs.

Refer to the *Fabric OS Administrator's Guide* for troubleshooting information.

Severity INFO

SULB-1010

Message `<timestamp>, [SULB-1010], <sequence-number>, AUDIT, INFO, <system-name>, Firmwarecommit failed (status=0x<error code>).`

Probable Cause Indicates the **firmwareCommit** command has failed. The error code provides debugging information. See Table 7 for more information.

Recommended Action If the failure is caused by an inconsistent filesystem, contact your switch service provider.

Severity INFO

SULB-1011

Message `<timestamp>, [SULB-1011], <sequence-number>,, INFO, <system-name>, Firmwaredownload command failed. <error string>.`

Probable Cause Indicates the **firmwareDownload** command has failed. The additional *state code* indicates where in the process it failed. *Status code* provides debugging information (see the tables in message 1109).

Recommended Action Run the **firmwareDownloadStatus** command for more information.

Refer to the Troubleshooting section of the *Fabric OS Administrator's Guide* for additional information.

Severity INFO

SULB-1017

Message `<timestamp>, [SULB-1017], <sequence-number>, AUDIT, ERROR, <system-name>, Firmwaredownload failed in slot <Slot number>.`

Probable Cause Indicates the **firmwareDownload** command has failed in the specified blade. The error may be caused by an inconsistent AP blade firmware stored on the active CP. It may also be caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended Action Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload**. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1018

Message `<timestamp>, [SULB-1018], <sequence-number>, AUDIT, ERROR, <system-name>, Firmwaredownload timed out in slot <Slot number>.`

Probable Cause Indicates there may be an error caused by the blade initialization issue after the new firmware is downloaded and the blade is rebooted. The error may also be caused by the internal Ethernet issue or by the persistent storage failure.

Recommended Action Run the **slotShow** command. If the blade is in FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload**. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1020

Message `<timestamp>, [SULB-1020], AUDIT, ERROR, <system-name>, New firmware failed to boot in slot <Slot number>.`

Probable Cause Indicates the BP blade is still running the old image even though it should reboot with the new image. This error may indicate that the new image has not been loaded correctly to the specified blade.

Recommended Action Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload** to the blade. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1021

Message `<timestamp>, [SULB-1021],<sequence-number>, AUDIT, WARNING, <system-name>, Firmware is being downloaded to the blade in slot <Slot number>.`

Probable Cause Indicates the firmware is being loaded to the indicated blade.

Recommended Action Run the **firmwareDownloadStatus** command to monitor the **firmwareDownload** progress. After it finishes, run the **firmwareShow** command to verify the firmware versions.

Severity WARNING

SULB-1022

Message `<timestamp>, [SULB-1022], <sequence-number>,, WARNING, <system-name>, The blade in slot <Slot number> has rebooted successfully with new firmware.`

Probable Cause Indicates that the blade in the specified slot has rebooted with new firmware. This is a normal step in the **firmwareDownload** process.

Recommended Action Run the **firmwareDownloadStatus** command to monitor the **firmwareDownload** progress.

Severity WARNING

SULB-1023

Message `<timestamp>, [SULB-1023], AUDIT, WARNING, <system-name>, The blade in slot <Slot number> has rebooted during firmwaredownload.`

Probable Cause Indicates there may be an error caused by an unexpected disruption of the **firmwareDownload** command, for example, by powering off and on of the indicated BP blade in the middle of a **firmwareDownload**. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended Action The **firmwareCommit** will be started automatically after the blade boots up to repair the secondary partition. If at the end of **firmwareCommit**, the blade firmware version is still inconsistent with the active CP firmware, **firmwareDownload** will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress. If the problem persists, contact your switch service provider.

Severity WARNING

SULB-1024

Message `<timestamp>, [SULB-1024], AUDIT, WARNING, <system-name>, Firmware commit has completed on the blade in slot <Slot number>.`

Probable Cause Indicates the **firmwareCommit** operation has completed on the specified blade.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. If the blade firmware is the same as the active CP firmware, **firmwareDownload** has completed successfully on the blade. However, if the **firmwareCommit** operation has been started to repair the secondary partition, at the end of **firmwareCommit**, the blade firmware version may still be inconsistent with the active CP firmware. In that case, **firmwareDownload** will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress.

Severity WARNING

SULB-1025

Message `<timestamp>, [SULB-1025], <sequence-number>,, WARNING, <system-name>, The blade in slot <Slot number> will reboot with the new firmware.`

Probable Cause Indicates new firmware has been downloaded to the specified AP blade and that the AP blade will reboot to activate it.

Recommended Action Wait for the blade to reboot.

Severity WARNING

SULB-1026

Message `<timestamp>, [SULB-1026], <sequence-number>, AUDIT, WARNING, <system-name>, Firmware commit operation started on the blade in slot <Slot number>.`

Probable Cause Indicates the **firmwareCommit** has started on the specified blade. The operation may be a normal part of **firmwareDownload**, or it may have started to repair the secondary partition of the blade if the secondary partition is corrupted.

Recommended Action No action is required.

Severity WARNING

SULB-1030

Message `<timestamp>, [SULB-1030], AUDIT, WARNING, <system-name>, The switch has rebooted during relocating the internal firmware image.`

Probable Cause Indicates there may be an error caused by an unexpected disruption of the **firmwareDownload** command, for example, by powering the switch off and on in the middle of a **firmwareDownload**. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended Action The **firmwareDownload** command will continue after the switch has rebooted. Run the **firmwareDownloadStatus** command to monitor progress. If the problem persists, contact your switch service provider.

Severity WARNING

SULB-1031

Message `<timestamp>, [SULB-1031], <sequence-number>, AUDIT, WARNING, <system-name>, The switch is relocating an internal firmware image.`

Probable Cause Indicates the switch has rebooted with the new firmware and is relocating the AP firmware.

Recommended Action Wait for the operation to complete.

Severity WARNING

SULB-1032

Message `<timestamp>, [SULB-1032], <sequence-number>, AUDIT, WARNING, <system-name>, Relocating an internal firmware image on the CP.`

Probable Cause Indicates the switch has started a firmware download to the co-CPU.

Recommended Action Wait for the operation to complete.

Severity WARNING

SULB-1033

Message `<timestamp>, [SULB-1033], <sequence-number>, AUDIT, WARNING, <system-name>, Switch has completed relocating the internal firmware image.`

Probable Cause Indicates the **firmwareDownload** process has completed normally on the switch.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. Run the **switchShow** command to make sure the switch is enabled.

Severity WARNING

SULB-1034

Message `<timestamp>, [SULB-1034], <sequence-number>, AUDIT, ERROR, <system-name>, Relocation of internal image timed out.`

Probable Cause Indicates there may be an error caused by the switch initialization issue after the internal image is relocated. It may also be caused by the internal Ethernet issue or by persistent storage failure.

Recommended Action Restart the switch. This will cause the internal image to be relocated again. Use the **firmwareDownloadStatus** command to monitor the progress. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1035

Message `<timestamp>, [SULB-1035], <sequence-number>, AUDIT, ERROR, <system-name>, An error has occurred during relocation of the internal image.`

Probable Cause Indicates an error has occurred during the relocation of the internal image. The error may be caused by inconsistent internal firmware image. It may also be caused by the internal Ethernet or persistent storage hardware failure.

Recommended Action Reset the switch. This will cause the internal image to be relocated again. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1036

Message

```
<timestamp>, [SULB-1036], <sequence-number>,, INFO, <system-name>, <The Version
being logged><Version String>.
```

Probable Cause Indicates the firmware version is running in the system. This is generally logged before download and after download of the firmware to store version information.

Recommended Action No action is required.

Severity INFO

SULB-1037

Message

```
<timestamp>, [SULB-1037], <sequence-number>, AUDIT, INFO, <system-name>, HCL
failed. Reboot the switch manually using the reboot command. However, it will
disrupt the FC traffic.
```

Probable Cause Indicates HCL has failed. Many reasons, such as domain not confirmed, can cause this failure.

Recommended Action Run the **reboot** command to reboot the switch manually.

Severity INFO

SULB-1038

Message

```
<timestamp>, [SULB-1038], WARNING, FIRMWARE, Co-CPU has not booted up properly.
Skip the firmwaredownload command on the co-CPU.
```

Probable Cause Indicates that the Main CPU cannot access the co-CPU to update the firmware on the co-CPU or run any other firmwaredownload command on the co-CPU. If firmwareDownload in progress it will continue without updating the co-CPU firmware.

Recommended Action After firmwaredownload completes, reboot the CP manually to bring up the co-CPU and run the **firmwareDownload** command again. If the problem persists, contact the service provider.

Severity WARNING

SULB-1039

Message `<timestamp>, [SULB-1039], INFO, FIRMWARE, CP has completed relocating the internal firmware image.`

Probable Cause Indicates that the firmwareDownload command process has been completed normally on the CP.

Recommended Action Run the **firmwareShow** command to verify the firmware versions.

Severity INFO

SULB-1040

Message `<timestamp>, [SULB-1040], INFO, WARNING, An error has occurred during relocation of the internal image on the CP.`

Probable Cause Indicates an error has occurred during the relocation of the internal image. The error may be caused by inconsistent internal firmware image. It may also be caused by the internal Ethernet failure.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. Run the **firmwareDownload** command again if the firmware is not updated.

This will cause the internal image to be relocated again. If the problem persists, contact your switch service provider.

Severity WARNING

Chapter

SWCH System Messages

98

SWCH-1001

Message `<timestamp>, [SWCH-1001], <sequence-number>,, ERROR, <system-name>, Switch is not in ready state - Switch enable failed switch status= 0x<switch status>, c_flags = 0x<switch control flags>.`

Probable Cause Indicates the switch is enabled before it is ready.

Recommended Action If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

SWCH-1002

Message `<timestamp>, [SWCH-1002], <sequence-number>,, INFO, <system-name>, Security violation: Unauthorized device <wwn name of device> tries to flogin to port <port number>.`

Probable Cause Indicates the device is not present in the authorized profile list.

Recommended Action Verify the device is authorized to log in to the switch. If the device is authorized, run the **secPolicyDump** command to verify whether the specified device world wide name (WWN) is listed. If it is not listed, run the **secPolicyAdd** command to add this device to an existing policy.

Severity INFO

SWCH-1003

Message `<timestamp>, [SWCH-1003], <sequence-number>,, ERROR, <system-name>, Slot ENABLED but Not Ready during recovery, disabling slot = <slot number>(<return value>).`

Probable Cause Indicates the slot state has been detected as inconsistent during failover or recovery.

Recommended Action On a Brocade 24000 or 48000 switch, run the **slotPowerOff** command and then the **slotPowerOn** command.

On a Brocade 7500 or AP7600 switch, reboot or power cycle the switch.

Severity ERROR

SWCH-1004

Message `<timestamp>, [SWCH-1004], <sequence-number>,, ERROR, <system-name>, Blade attach failed during recovery, disabling slot = <slot number>.`

Probable Cause Indicates a blade has failed during failover or recovery.

Recommended Action On a Brocade 24000 or 48000 switch, run the **slotPowerOff** command and then the **slotPowerOn** command.

On a Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, or AP7600 switch, reboot or power cycle the switch

Severity ERROR

SWCH-1005

Message `<timestamp>, [SWCH-1005], <sequence-number>,, ERROR, <system-name>, Diag attach failed during recovery, disabling slot = <slot number>.`

Probable Cause Indicates the Diag blade attach has failed during failover or recovery.

Recommended Action On a Brocade 24000 or 48000 switch, run the **slotPowerOff** command and then the **slotPowerOn** command.

On a Brocade 200E, 3250, 3850, 3900, 4012, 4016, 4018, 4020, 4024, 4100, 4900, 5000, 7500, or AP7600 switch, reboot or power cycle the switch.

Severity ERROR

SWCH-1006

Message `<timestamp>, [SWCH-1006], <sequence-number>,, WARNING, <system-name>, HA state out of sync: Standby CP (ver = <standby SWC version>) does not support NPIV functionality. (active ver = <active SWC version>, NPIV devices = <'1' if NPIV devices exist; Otherwise '0'. >).`

Probable Cause Indicates the standby control processor (CP) does not support N_Port ID Virtualization (NPIV) functionality, but the switch has some NPIV devices logged into the fabric.

Recommended Action Load a firmware version on standby that supports NPIV functionality, using the **firmwareDownload** command.

Severity WARNING

SWCH-1007

Message `<timestamp>, [SWCH-1007], <sequence-number>,, WARNING, <system-name>, Switch port <port number> disabled due to \"<disable reason>\".`

Probable Cause Indicates the switch port is disabled due to the reason displayed in the message.

Recommended Action Based on the disable reason displayed, proper corrective action may to be required to restore the port.

If the disable reason is due to insufficient frame buffers, reduce the distance or speed settings for the port to reduce the buffer requirement of the link. Alternatively, one or more ports in the port group must be disabled to make more buffers available for the link.

Refer to the *Fabric OS Administrator's Guide* for more information about buffers.

Severity WARNING

SWCH-1008

Message

```
<timestamp>, [SWCH-1008], <sequence-number>,, WARNING, <system-name>, <area
string> are port swapped on ports that do not support port swap. Slot <slot
number> will be faulted.
```

Probable Cause Indicates the blade is enabled with the port configuration that does not support port swap.

Recommended Action Replace the blade with ports that support port swap. Then swap the ports back to the ports default area.

Refer to the *Fabric OS Administrator's Guide* for more information on port swapping.

Severity WARNING

SWCH-1009

Message

```
<timestamp>, [SWCH-1009], <sequence-number>,, WARNING, <system-name>, Shared area
having Trunk Area (TA) enabled on slot <slot number>. Shared areas that have TA
enabled will be persistenly disabled.
```

Probable Cause Indicates the blade is enabled with a port configuration that had Trunk Area previously enabled on a shared area port.

Recommended Action You must disable Trunk Area on ports that had Trunk Area enabled previously.

Refer to the *Fabric OS Administrator's Guide* for more information.

Severity WARNING

SWCH-1010

Message

```
<timestamp>, [SWCH-1010], <sequence-number>,, WARNING, <system-name>, Trunk Area
(TA) enabled on slot <slot number> with switch not in PID format 1.  TA enabled
ports will be persistently disabled.
```

Probable Cause Indicates the blade is enabled with the port configuration that had Trunk Area enabled previously.

Recommended Action You must disable Trunk Area on ports that had Trunk Area enabled previously.

Refer to the *Fabric OS Administrator's Guide* for more information.

Severity WARNING

SWCH-1011

Message `<timestamp>, [SWCH-1011], <sequence-number>,, WARNING, <system-name>, HA state out of sync: Standby CP (ver = <standby SWC version>) does not support Trunk Area functionality. (active ver = <active SWC version>, Trunk Area enabled on switch = <'1' if Trunk Area ports exist; Otherwise '0'>).`

Probable Cause Indicates the standby control processor (CP) does not support Trunk Area functionality, but the switch has some ports with Trunk Area enabled.

Recommended Action Load a firmware version on standby that supports Trunk Area functionality, using the **firmwareDownload** command.

Severity WARNING

SWCH-1012

Message `<timestamp>, [SWCH-1012], <sequence-number>,, INFO, <system-name>, Trunk Area (<trunk area>) has been enabled for one or more ports).`

Probable Cause Indicates that a Trunk Area has been enabled for one or more ports and the configuration file has been updated.

Recommended Action No action is required.

Severity INFO

SWCH-1013

Message `<timestamp>, [SWCH-1013], <sequence-number>,, INFO, <system-name>, Trunk Area has been disabled for one or more ports.`

Probable Cause Indicates that a Trunk Area assignment has been disabled for one or more ports and the configuration file has been updated.

Recommended Action No action is required.

Severity INFO

SWCH-1014

Message `<timestamp>, [SWCH-1014], <sequence-number>,, INFO, <system-name>, All Trunk Areas have been disabled.`

Probable Cause Indicates that all Trunk Areas have been disabled and the configuration file has been updated.

Recommended Action No action is required.

Severity INFO

SWCH-1015

Message `<timestamp>, [SWCH-1015], <sequence-number>,, WARNING, <system-name>, <Function name> <Description of problem>.`

Probable Cause Indicates that an internal problem has been detected by the software. This is usually an internal Fabric OS problem or due to file corruption.

Recommended Action Restart or power cycle the switch

If the message persists, run the **firmwareDownload** command to update the firmware.

Severity WARNING

SWCH-1016

Message `<timestamp>, [SWCH-1016], <sequence-number>,, INFO, <system-name>, Device <wwn name of device>fdiscs to port <port number>. Static persistent PID set and area requested not assigned to the device. Reject FDISC.`

Probable Cause Indicates static persistent PID is set and the area requested is not assigned to the device.

Recommended Action This is a NPIV device and static peristent PID is set on it, we are not able to assign the area requested. Remove the static binding to have the device come up with a different area and run the **wwnaddress –unbind wwn** command.

Severity INFO

SWCH-1017

Message `<timestamp>, [SWCH-1017], <sequence-number>,, INFO, <system-name>, Device <wwn name of device> tries to flogi to port <port number>, reject FLOGI as persistent PID is set on the Loop device.`

Probable Cause Indicates persistent PID is set and static Persistent PID is not supported on the Loop device.

Recommended Action This is a LOOP device and peristent PID is set on it. This is not a supported configuration. Remove the WWN-PID binding and re-enable the port and then run the **wwnaddress –unbind wwn** command.

Severity INFO

SWCH-1019

Message `<timestamp>, [SWCH-1019], <sequence-number>,, INFO, <system-name>, Device <wwn name of device> tries to flogi, reject FLOGI as persistent PID is set on device and port <port number> has user area <area> bound to it.`

Probable Cause Indicates a WWN-PID and PortAddress binding collision.

Recommended Action The Peristent PID is set on the device and requested area cannot be assigned because it is user bound to a different port. Remove the WWN-PID binding or remove portAddress binding and re-enable the port and then run the **wwnaddress –unbind wwn** command or the **portaddress –unbind slot/port** command.

Severity INFO

SWCH-1020

Message `<timestamp>, [SWCH-1020], <sequence-number>,, WARNING, <system-name>,HA state out of sync: Standby CP (ver = <standby SWC version>) does not support QOS links to AG(Active CP version = <active SWC version>).`

Probable Cause Indicates the standby control processor (CP) does not support links to AG running QOS.

Recommended Action Load a firmware version on the standby CP that supports QOS links to AG, using the **firmwareDownload** command.

Severity WARNING

SWCH-1021

Message `<timestamp>, [SWCH-1021], <sequence-number>,, WARNING, <system-name>, HA state out of sync: Standby CP (ver = <standby SWC version>) does not support Dynamic area on default switch (Active CP version = <active SWC version>).`

Probable Cause Indicates the standby control processor (CP) does not support dynamic area on default switch.

Recommended Action Load a firmware version on the standby CP that supports dynamic area on default switch, using the **firmwareDownload** command.

Severity WARNING

Chapter

SYSC System Messages

99

SYSC-1001

Message `<timestamp>, [SYSC-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, Failed to run <Name of program that could not be run (string)>:<System internal error message (string)>.`

Probable Cause Indicates that during the boot sequence, one of the programs does not run on the system.

Recommended Action If the message is reported during a restart after new firmware has been loaded, try reloading the firmware using the **firmwareDownload** command.

If the message persists, there might be a conflict between the two versions of firmware or the nonvolatile storage might be corrupted. Run **supportFtp** (as needed) to set up automatic FTP transfers and run the **supportSave** command then contact your switch service provider.

Severity CRITICAL

SYSC-1002

Message `<timestamp>, [SYSC-1002], <sequence-number>, FFDC, CRITICAL, <system-name>, Switch bring-up timed out.`

Probable Cause Indicates the system has timed out during a restart or failover sequence, waiting for one or more programs to register with system services or to fail over to active status.

Recommended Action The switch is in an inconsistent state and can be corrected only by a restart or power cycle. Before restarting the chassis, record the firmware version on the switch or control processor (CP) and run the **haDump** command. If this is a dual-CP switch, then gather the output from the CP in which this log message appeared.

Severity CRITICAL

SYSC-1003

Message `<timestamp>, [SYSC-1003], <sequence-number>, FFDC, CRITICAL, <system-name>, Chassis config option <Option number read from the chassis option storage device> is not supported by CP Blade with ID <Blade ID (platform) number from the Active CP>. Change the chassis configuration <Steps to change chassis configuration>`

Probable Cause Indicates that on system startup, the option configuration file corresponding to the **chassisConfig** option read could not be found. This indicates that option is not supported on this platform running this version of the firmware.

It could also indicate that the current option number could not be read from the chassis option storage device (the world wide name (WWN) card).

This message occurs only on the Brocade 24000 and 48000.

Recommended Action As indicated in the message, run the **chassisConfig** command to change to one that is valid on this platform running this firmware. Note that the **chassisConfig** option 1 should be valid for all platforms running any valid firmware.

Severity CRITICAL

SYSC-1004

Message `<timestamp>, [SYSC-1004], <sequence-number>,, INFO, <system-name>, Daemon <Daemon name to restart> restart successful`

Probable Cause Indicates that a terminated daemon is being restarted by the system automatically.

Recommended Action Use the **supportSave** command to gather troubleshooting data.

Severity INFO

SYSC-1005

Message `<timestamp>, [SYSC-1005], <sequence-number>,, WARNING, <system-name>, Daemon <Daemon name to restart> is not restarted (Reason: <Restart failure reason>)`

Probable Cause Indicates a terminated daemon has not restarted, either a restart limit has been reached or a restart action has failed.

Recommended Action Use the **supportSave** command to gather troubleshooting data. Issue a **reboot** or **haFailover** command to recover the system and limit the traffic disruption.

Severity WARNING

Chapter

SYSM System Messages

100

SYSM-1001

Message `<timestamp>, [SYSM-1001], <sequence-number>, FFDC, CRITICAL, <system-name>, No memory.`

Probable Cause Indicates the switch has run out of system memory.

Recommended Action Run the **memShow** command to view the switch memory usage.

Restart or power cycle the switch.

Run the **supportFtp** command to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

SYSM-1002

Message `<timestamp>, [SYSM-1002], <sequence-number>,, INFO, <system-name>, <number>, Switch: <Switch number>`

Probable Cause Indicates a user has executed either the **switchShutdown** or **switchReboot** command. All services are brought down for a logical switch.

Recommended Action No action is required if the **switchShutdown** or **switchReboot** command was executed intentionally. If the **switchShutdown** command was run, you must run the **switchStart** command to restart traffic on the logical switch.

Severity INFO

SYSM-1003

Message `<timestamp>, [SYSM-1003], <sequence-number>,, INFO, <system-name>, <number>, Switch: <start reason>`

Probable Cause Indicates the user executed the **switchStart** or **switchReboot** command. This indicates that all services are brought back up after a temporary shutdown of that logical switch.

Recommended Action No action is required if the **switchStart** command was executed intentionally. Because reinitializing a switch is a disruptive operation and can stop I/O traffic, you might have to stop and restart the traffic during this process.

Severity INFO

SYSM-1004

Message `<timestamp>, [SYSM-1004], <sequence-number>,, ERROR, <system-name>, Failed to retrieve current chassis configuration option, ret=<Unknown>`

Probable Cause Indicates there was a failure to read configuration data from the WWN card.

Recommended Action Verify that the world wide name (WWN) card is present and operational and that the affected control processor (CP) is properly seated in its slot.

Severity ERROR

SYSM-1005

Message `<timestamp>, [SYSM-1005], <sequence-number>, FFDC, CRITICAL, <system-name>, CP blade in slot <Slot number> failed to retrieve current chassis type.`

Probable Cause Indicates there was a failure to read the chassis type from the system.

Recommended Action Verify the control processor (CP) blade is operational and is properly seated in its slot.

Severity CRITICAL

SYSM-1006

Message `<timestamp>, [SYSM-1006], <sequence-number>, FFDC, CRITICAL, <system-name>, CP blade in slot <Slot number> is incompatible with the chassis type.`

Probable Cause Indicates this chassis type is not compatible with the control processor (CP) blade.

Recommended Action Use the CP blade on a compatible chassis.

Severity CRITICAL

SYSM-1007

Message `<timestamp>, [SYSM-1007], <sequence-number>,, WARNING, <system-name>, PERMITTING USE OF INCOMPATIBLE CHASSIS FOR CP IN SLOT <Slot number>. DATA ERRORS MAY RESULT.`

Probable Cause Indicates overriding the incompatible control processor (CP)/chassis check.

Recommended Action Delete the /var/chassis_backplane_override file and restart the CP.

Severity WARNING

Chapter

TAPE System Messages

101

TAPE-1001

Message `<timestamp>, [TAPE-1001], <sequence-number>, FFDC, INFO, <system-name>, Key acquisition for <Pool or Container><Begins or Complete>.`

Probable Cause Indicates that the key acquisition for the pool or the container has begun or is complete.

Recommended Action No action is required.

Severity INFO

101 TAPE-1001

Chapter

TRCE System Messages

102

TRCE-1001

Message `<timestamp>, [TRCE-1001], <sequence-number>,, WARNING, <system-name>, Trace dump available< optional slot indicating on which slot the dump occurs >! (reason: <Text explanation of what triggered the dump. (PANIC DUMP, WATCHDOG EXPIRED, MANUAL, TRIGGER)>)`

Probable Cause Indicates that trace dump files have been generated on the switch or the indicated slot. The reason field indicates the cause for generating the dump as one of the following:

- PANICDUMP generated by panic dump
- WATCHDOG EXPIRED generated by hardware watchdog expiration
- MANUAL generated by the **tracedump -n** command
- TRIGGER when triggered by a specific Message ID generated by CRITICAL RASLog message or RASLog message trigger setup using the **traceTrig** command.

Recommended Action Run the **supportFtp** command to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

TRCE-1002

Message `<timestamp>, [TRCE-1002], <sequence-number>,, INFO, <system-name>, Trace dump< optional slot indicating on which slot the dump occurs > automatically transferred to FTP address ' <FTP target designated by user> '.`

Probable Cause Indicates that a trace dump has occurred on the switch or the indicated slot and it is successfully transferred from the switch automatically.

Recommended Action No action is required.

Severity INFO

TRCE-1003

Message `<timestamp>, [TRCE-1003], <sequence-number>,, ERROR, <system-name>, Trace dump< optional slot indicating on which slot the dump occurs > was not transferred due to FTP error.`

Probable Cause Indicates that a trace dump has been created on the switch or the indicated slot but is not automatically transferred from the switch due to an FTP error, such as a wrong FTP address, FTP site down, or network down.

Recommended Action If the message persists, run the **supportFtp** command to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

TRCE-1004

Message `<timestamp>, [TRCE-1004], <sequence-number>,, WARNING, <system-name>, Trace dump< optional slot indicating on which slot the dump occurs > was not transferred because trace auto-FTP disabled.`

Probable Cause Indicates that trace dump files have been created on the switch or the indicated slot but are not automatically transferred from the switch because auto-FTP is disabled.

Recommended Action Run the **supportFtp** command to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

TRCE-1005

Message `<timestamp>, [TRCE-1005], <sequence-number>,, ERROR, <system-name>, FTP Connectivity Test failed due to error.`

Probable Cause Indicates that the connectivity test to the FTP host fails, because of an FTP error such as a wrong FTP address, an FTP site down, or the network being down.

Recommended Action Run the **supportFtp** command to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

TRCE-1006

Message `<timestamp>, [TRCE-1006], <sequence-number>,, INFO, <system-name>, FTP Connectivity Test succeeded to FTP site ' <FTP target configured by users.> '.`

Probable Cause Indicates that a connectivity test to the FTP host has succeeded. This feature is enabled by the **supportFtp -t** command.

Recommended Action No action is required.

Severity INFO

TRCE-1007

Message `<timestamp>, [TRCE-1007], <sequence-number>,, ERROR, <system-name>, Notification of this CP has failed. Parameters temporarily out of sync with other CP.`

Probable Cause Indicates that the active CP is unable to alert the standby CP of a change in trace status. This message is only applicable to the Brocade 24000, and 48000.

Recommended Action This message is often transitory. Wait for a few minutes and retry the command.

If the message persists, run the **supportFtp** command to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

TRCE-1008

Message `<timestamp>, [TRCE-1008], <sequence-number>, FFDC, CRITICAL, <system-name>, Unable to load trace parameters.`

Probable Cause Indicates that the active CP is unable to read stored trace parameters.

Recommended Action Restart the CP (dual-CP system) or restart the switch.

If the message persists, run the **supportFtp** command to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity CRITICAL

TRCE-1009

Message `<timestamp>, [TRCE-1009], <sequence-number>,, ERROR, <system-name>, Unable to alert active CP that a dump has occurred.`

Probable Cause Indicates that the standby CP is unable to communicate trace information to active CP. This message is only applicable to the Brocade 24000 and 48000.

Recommended Action Run the **haShow** command to verify that the current CP is standby and the active CP is active.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

TRCE-1010

Message `<timestamp>, [TRCE-1010], <sequence-number>,, ERROR, <system-name>, Traced fails to start`

Probable Cause Indicates that the trace daemon (traced), used for transferring trace files, failed to start. The trace capability within the switch is unaffected. The traced facility is normally restarted automatically by the system after a brief delay.

Recommended Action If the message persists, restart the CP (dual-CP system) or restart the switch.

Run the **supportFtp** command to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

TRCE-1011

Message `<timestamp>, [TRCE-1011], <sequence-number>,, INFO, <system-name>, Trace dump manually transferred to target ' <optional string to indicate which slot the dump is ftped out.> ': <result>.`

Probable Cause Indicates that a manual transfer of trace dump files has occurred.

Recommended Action No action is required.

Severity INFO

TRCE-1012

Message `<timestamp>, [TRCE-1012], <sequence-number>,, WARNING, <system-name>, The system was unable to retrieve trace information from slot <Slot number of the blade the attempt was made on>.`

Probable Cause Indicates that communication between the main system and the indicated slot is unavailable.

Recommended Action Make sure the blade is enabled and retry the command. If the blade is already enabled, run the **supportSave** command and contact your switch service provider.

Severity WARNING

Chapter

TRCK System Messages

103

TRCK-1001

Message `<timestamp>, [TRCK-1001], <sequence-number>,, INFO, <system-name>, Successful login by user <User>.`

Probable Cause Indicates the track change feature has recorded a successful login.

Recommended Action No action is required.

Severity INFO

TRCK-1002

Message `<timestamp>, [TRCK-1002], <sequence-number>,, INFO, <system-name>, Unsuccessful login by user <User> after <login_fail_cnt> overall login failure attempts.`

Probable Cause Indicates the track change feature has recorded a failed login. This occurs if the user name or password is incorrect.

Recommended Action This message indicates a typing error by the user. If this message occurs repeatedly, it might indicate an unauthorized user trying to gain access to a switch. When Secure mode is enabled on the fabric, the IP address of a failed login is reported to the error log.

Severity INFO

TRCK-1003

Message `<timestamp>, [TRCK-1003], <sequence-number>,, INFO, <system-name>, Logout by user <User>.`

Probable Cause Indicates the track change feature has recorded a successful logout.

Recommended Action No action is required.

Severity INFO

TRCK-1004

Message `<timestamp>, [TRCK-1004], <sequence-number>,, INFO, <system-name>, Config file change from task:<task>.`

Probable Cause Indicates the track change feature recorded a configuration change for the switch. The track change feature records any change to the configuration file in nonvolatile memory, including a **configDownload** command. This message is not generated for a **configUpload** command. All configuration changes occur through the PDM server, so the PDMIPC is the only task possible.

Recommended Action No action is required. Run the **configShow** command to view the configuration file.

Severity INFO

TRCK-1005

Message

```
<timestamp>, [TRCK-1005], <sequence-number>,, INFO, <system-name>, Track-changes
on.
```

Probable Cause Indicates the track change feature has been enabled.

Recommended Action No action is required. Run the **trackChangesSet 0** command to disable the track change feature.

Severity INFO

TRCK-1006

Message

```
<timestamp>, [TRCK-1006], <sequence-number>,, INFO, <system-name>, Track-changes
off.
```

Probable Cause Indicates the track change feature has been disabled.

Recommended Action No action is required. Run the **trackChangesSet 1** command to enable the track changes feature.

Severity INFO

Chapter

TS System Messages

104

TS-1001

Message `<timestamp>, [TS-1001], <sequence-number>,, WARNING, <system-name>, NTP Query failed: <error code>.`

Probable Cause Indicates a network time protocol (NTP) query to the configured external clock server failed. Local clock time on the principal or primary fabric configuration server (FCS) switch is used for fabric synchronization.

This might be logged during temporary operational issues such as IP network connection issues to the external clock server. If it does not recur, it can be ignored.

Recommended Action Verify the configured external clock server is available and functional. If that external clock server is not available, choose another.

Severity WARNING

TS-1002

Message `<timestamp>, [TS-1002], <sequence-number>,, INFO, <system-name>, < Type of clock server used > Clock Server used instead of < Type of clock server configured >: locl: 0x<code> remote: 0x<code>.`

Probable Cause Indicates the fabric time synchronization distributed from the principal or primary fabric configuration server (FCS) switch was not sourced from the *Type of clock server configured*, instead, an alternate server was used, indicated by *Type of clock server used*. The type of clock server used or configured might be either one of the following:

- LOCL
  Local clock on the principal or primary FCS switch
- External
  External NTP server address configured

This might be logged during temporary operational issues such as IP network connection issues to the external clock server or if the fabric is configured for external time synchronization but the principal or primary FCS does not support the feature. If the message does not recur, it should be ignored.

Recommended Action Run the **tsClockServer** command to verify that the principal or primary FCS switch has the clock server IP configured correctly. Verify this clock server is accessible to the switch and functional. If the principal or primary FCS does not support the feature, either choose a different switch for the role or reset the clock server to LOCL.

Severity INFO

TS-1006

Message `<timestamp>, [TS-1006], <sequence-number>,, INFO, <system-name>, <message>.`

Probable Cause Indicates a time service event is occurring or has failed. The message might be one of the following:

- Init failed. Time Service exiting
  Probable Cause: Initialization error, Time Server exits.
- Synchronizing time of day clock
  Probable Cause: Usually logged during temporary operational issues when the clock goes out of synchronization: For example, when a time update packet is missed due to fabric reconfiguration or role change of the principal or primary fabric configuration server (FCS) switch. If the message does not recur, it should be ignored.
- Validating time update
  Probable Cause: Usually logged during temporary operational issues when a time update packet cannot be validated in a secure fabric. For example, during fabric reconfiguration or role change of the primary FCS switch. If the message does not recur, it should be ignored.

Recommended Action No action is required.

Severity INFO

TS-1007

Message `<timestamp>, [TS-1007], <sequence-number>,, WARNING, <system-name>, <message>.`

Probable Cause Indicates a switch is trying to set the tsclockserver, which is not the primary fabric configuration server (FCS) across the fabric. A consistent FCS policy must be implemented across the fabric.

Recommended Action Verify the FCS policy is consistent across the fabriclog_ts.xml.

Severity WARNING

TS-1008

Message `<timestamp>, [TS-1008], <sequence-number>,, WARNING, <system-name>, <New clock server used> Clock Server used instead of <Old server configured>.`

Probable Cause Indicates there is a change in the source of fabric time synchronization distributed from the principal or primary fabric configuration server (FCS) switch. Another clock server in the list of clock servers configured is being used. This happens when the network time protocol (NTP) query to the current active external clock server fails.

Recommended Action No action is required.

Severity WARNING

Chapter

UCST System Messages

105

UCST-1003

Message `<timestamp>, [UCST-1003], <sequence-number>,, INFO, <system-name>, Duplicate Path to Domain <domain ID>, Output Port = <port number>, PDB pointer = 0x<value>`

Probable Cause Indicates the duplicate paths were reported to the specified domain from the specified output port. The path database (PDB) pointer is the address of the path database and provides debugging information.

Recommended Action No action is required.

Severity INFO

UCST-1007

Message `<timestamp>, [UCST-1007], <sequence-number>, FFDC, CRITICAL, <system-name>, Inconsistent route detected: Port = <port number>, should be <port number>`

Probable Cause Indicates the switch detected an inconsistency in the routing database between the routing protocol and the hardware configuration. The first port number displayed is what the hardware has configured and the second port number displayed is what the protocol is using.

Recommended Action Run the **switchDisable** command and then the **switchEnable** command to reset the routing database. Run the **uRouteShow** command to display the new routing tables.

Severity CRITICAL

UCST-1020

Message `<timestamp>, [UCST-1020], <sequence-number>,, WARNING, <system-name>, Static route (input-area: <port number>, domain: <domain ID> output-area: <port number>) has been ignored due to platform limitation.`

Probable Cause Indicates the configured static route cannot be applied to the routing database due to a platform limitation.

Recommended Action No action is required.

Severity WARNING

UCST-1025

Message `<timestamp>, [UCST-1025], <sequence-number>,, INFO, <system-name>, In-order delivery option has been enabled with Lossless-DLS option.`

Probable Cause Indicates the IOD option has been enabled for the switch. This option guarantees in-order delivery of frames during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1026

Message `<timestamp>, [UCST-1026], <sequence-number>,, INFO, <system-name>, LossLess-DLS option has been enabled.`

Probable Cause Indicates that the *NoFrameDrop* option is enabled. This will help minimize frame loss during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1027

Message `<timestamp>, [UCST-1027], <sequence-number>,, INFO, <system-name>, LossLess-DLS option has been disabled.`

Probable Cause Indicates that the *NoFrameDrop* option is disabled. This may cause higher frame loss during topology changes.

Recommended Action No action is required.

Severity INFO

Chapter

UPTH System Messages

106

UPTH-1001

Message `<timestamp>, [UPTH-1001], <sequence-number>,, WARNING, <system-name>, No minimum cost path in candidate list.`

Probable Cause Indicates the specified switch is unreachable because no minimum cost path (FSPF UPATH) exists in the candidate list (domain ID list).

Recommended Action No action is required. This will end the current SPF computation.

Severity WARNING

UPTH-1002

Message `<timestamp>, [UPTH-1002], <sequence-number>,, WARNING, <system-name>, Domain <domain ID> is unreachable because the enabled TI zone is not compatible with the fabric configuration.`

Probable Cause Indicates the specified switch is unreachable because of the TI zone and the fabric configuration incompatibility.

Recommended Action Clear all TI zones and refer to the *TI zone user manual* for instructions on how to create a valid TI zone for your fabric configuration.

Severity WARNING

Chapter

WEBD System Messages

107

WEBD-1001

Message `<timestamp>, [WEBD-1001], <sequence-number>,, WARNING, <system-name>, Missing or Invalid Certificate file -- HTTPS is configured but could not be started.`

Probable Cause Indicates the SSL certificate file is either invalid or absent.

Recommended Action Install a valid key file.

Severity WARNING

WEBD-1002

Message `<timestamp>, [WEBD-1002], <sequence-number>,, WARNING, <system-name>, Missing or Invalid Key file -- HTTPS is configured but could not be started.`

Probable Cause Indicates the SSL key file is either invalid or absent.

Recommended Action Install a valid key file.

Severity WARNING

WEBD-1004

Message `<timestamp>, [WEBD-1004], <sequence-number>,, INFO, <system-name>, HTTP server and weblinker process will be restarted due to configuration change.`

Probable Cause Indicates the HTTP server configuration has changed.

Recommended Action No action is required.

Severity INFO

WEBD-1005

Message `<timestamp>, [WEBD-1005], <sequence-number>,, WARNING, <system-name>, HTTP server and weblinker process will be restarted for logfile truncation.`

Probable Cause Indicates the size of the HTTP log file exceeded the maximum limit.

Recommended Action No action is required.

Severity WARNING

WEBD-1006

Message `<timestamp>, [WEBD-1006], <sequence-number>,, INFO, <system-name>, HTTP server and weblinker restarted due to logfile truncation.`

Probable Cause Indicates the size of the HTTP log file exceeded the maximum limit.

Recommended Action No action is required.

Severity INFO

WEBD-1007

Message `<timestamp>, [WEBD-1007], <sequence-number>,, INFO, <system-name>, HTTP server and weblinker process will be restarted due to change of IP Address.`

Probable Cause Indicates the IP address of the switch changed and the HTTP server is restarted.

Recommended Action No action is required.

Severity INFO

WEBD-1008

Message `<timestamp>, [WEBD-1008], <sequence-number>, FFDC, WARNING, <system-name>, HTTP server and weblinker process cannot be started.`

Probable Cause Indicates a rare error condition, where the built-in recovery process has failed to restore HTTP services. The problem often results from invalid configuration of SSL certificates, but there can be more than one reason for such a failure.

Recommended Action Verify the certification file because there may be a mismatch involved.

Severity WARNING

Chapter

XTUN System Messages

108

XTUN-1000

Message `<timestamp>, [XTUN-1000], <sequence-number>,, ERROR, <system-name>, Missed Data frame:I/T/L:<FC Initiator ID> <FC Target ID> <FCP Logical Unit Number>.`

Probable Cause Indicates a missed frame with one or more FCP data information units during a SCSI write or read operation.

Recommended Action If there was an unexpected job failure associated with this event, contact your customer support for assistance.

Severity ERROR

XTUN-1001

Message `<timestamp>, [XTUN-1001], <sequence-number>,, ERROR, <system-name>, Memory allocation failed.`

Probable Cause Indicates a memory allocation failure.

Recommended Action Contact your customer support for assistance.

Severity ERROR

XTUN-1002

Message `<timestamp>, [XTUN-1002], <sequence-number>,, ERROR, <system-name>, Exchange timeout:I/T/L:<FC Initiator ID> <FC Target ID> <FCP Logical Unit Number>.`

Probable Cause Indicates that the FCP exchange has timed out.

Recommended Action If there was an unexpected job failure associated with this event, contact your customer support for assistance.

Severity ERROR

XTUN-1003

Message `<timestamp>, [XTUN-1003], <sequence-number>,, ERROR, <system-name>, Message Transmission failed:I/T/L:<FC Initiator ID> <FC Target ID> <FCP Logical Unit Number> <Error return value>.`

Probable Cause Indicates a message transmission failure.

Recommended Action If there was an unexpected job failure associated with this event, contact your customer support for assistance.

Severity ERROR

XTUN-1004

Message `<timestamp>, [XTUN-1004], <sequence-number>,, ERROR, <system-name>, Exchange aborted:I/T/L:<FC Initiator ID> <FC Target ID> <FCP Logical Unit Number>.`

Probable Cause Indicates that the FCP exchange has been aborted by the Initiator.

Recommended Action If there was an unexpected job failure associated with this event, contact your customer support for assistance.

Severity ERROR

XTUN-1998

Message `<timestamp>, [XTUN-1998], <sequence-number>,, INFO, <system-name>, FTRACE buffer <FTRACE Trace Buffer Number> has been cleared.`

Probable Cause Indicates that a CLI command caused the trace buffer to be put back into the FTRACE free pool.

Recommended Action No action is required.

Severity INFO

XTUN-1999

Message `<timestamp>, [XTUN-1999], <sequence-number>,, WARNING, <system-name>, FTRACE buffer <FTRACE Trace Buffer Number> has been triggered.`

Probable Cause Indicates that a programmed trigger event has been detected.

Recommended Action If there was an unexpected job failure associated with this event, contact your customer support for assistance.

Severity WARNING

XTUN-2000

Message `<timestamp>, [XTUN-2000], <sequence-number>,, INFO, <system-name>, FCIP Tunnel <Tunnel Number> UP.`

Probable Cause Indicates that the specified FCIP tunnel is up.

Recommended Action No action is required.

Severity INFO

XTUN-2001

Message `<timestamp>, [XTUN-2001], <sequence-number>,, ERROR, <system-name>, FCIP Tunnel <Tunnel Number> DOWN <Reason>.`

Probable Cause Indicates that the specified tunnel has gone down.

Recommended Action If the tunnel has not been administratively disabled or deleted, a possible network error or disruption has occurred.

Severity ERROR

XTUN-2002

Message `<timestamp>, [XTUN-2002], <sequence-number>,, INFO, <system-name>, FCIP Tunnel <Tunnel Number> Circuit <Circuit Number> UP.`

Probable Cause Indicates that the specified circuit is up.

Recommended Action No action is required.

Severity INFO

XTUN-2003

Message `<timestamp>, [XTUN-2003], <sequence-number>,, ERROR, <system-name>, FCIP Tunnel <Tunnel Number> Circuit <Circuit Number> DOWN <Reason>.`

Probable Cause Indicates that the specified circuit has gone down. The tunnel will also be down if this is the last circuit available.

Recommended Action If the tunnel or circuit has not been administratively disabled or deleted, a possible network error or disruption has occurred.

Severity ERROR

XTUN-2004

Message `<timestamp>, [XTUN-2004], <sequence-number>,, INFO, <system-name>, FCIP Tunnel <Tunnel Number> <Priority Class> Pri QoS UP.`

Probable Cause Indicates that the specified quality of service for this tunnel is up. This applies to the data classes only. When the f-class comes online, the tunnel itself is marked as up.

Recommended Action No action is required.

Severity INFO

XTUN-2005

Message `<timestamp>, [XTUN-2005], <sequence-number>,, INFO, <system-name>, FCIP Tunnel <Tunnel Number> <Priority Class> Pri QoS DOWN <Reason>.`

Probable Cause Indicates that the specified quality of service has gone down. This applies to the data classes only. If the f-class goes down, the tunnel itself is marked as down.

Recommended Action If the tunnel or circuit has not been administratively disabled or deleted, a possible network error or disruption has occurred.

Severity INFO

Chapter

ZEUS System Messages

109

ZEUS-1001

Message `<timestamp>, [ZEUS-1001], <sequence-number>,, ERROR, <system-name>, Port <port number> port fault. Please change the SFP or check cable.`

Probable Cause Indicates a deteriorated small form-factor pluggable (SFP), an incompatible SFP pair, or a faulty cable between peer ports.

Recommended Action Verify if you are using a compatible SFPs on the peer ports. Determine whether the SFPs have deteriorated and the Fibre Channel cable is faulty. Replace the SFPs or cable if necessary.

Severity ERROR

Chapter

ZOLB System Messages

110

ZOLB-1001

Message

```
<timestamp>, [ZOLB-1001], <sequence-number>,, ERROR, <system-name>, ZONELIB
<error message>
```

Probable Cause

Indicates there was an internal timeout on the inter process communication (IPC) between the name server (NS) and the zoning modules. This usually indicates that the system was busy.

Recommended Action

This message generates core dump files of the related modules (zoned, nsd, rcsd).

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command to save these core files and contact your switch service provider.

Severity

ERROR

Chapter

ZONE System Messages

111

ZONE-1002

Message `<timestamp>, [ZONE-1002], <sequence-number>,, WARNING, <system-name>, WWN zoneTypeCheck or zoneGroupCheck warning(<warning string>) at port(<port number>).`

Probable Cause Indicates a zone filter or zone group check failure occurred. The frame filter logic reported a failure when creating or adding zone groups during port login (PLOGI) trap processing. This messages usually indicates problems when adding content-addressable memory (CAM) entries before the filter setup.

Recommended Action If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

ZONE-1003

Message `<timestamp>, [ZONE-1003], <sequence-number>,, WARNING, <system-name>, zone(<current zone>) contains (<domain id>, <port number>) which does not exist.`

Probable Cause Indicates the port zone member that is targeted for the local switch contains a non-existent port. The effective zoning configuration (displayed in the error message) contains a port number that is out of range.

Recommended Action Edit the zone database and change the port number to a viable value in the effective configuration.

Severity WARNING

ZONE-1004

Message `<timestamp>, [ZONE-1004], <sequence-number>,, INFO, <system-name>, port <port number> (<port number (hex)>) enforcement changed to Session Based HARD Zoning.`

Probable Cause Indicates the zoning enforcement has changed to session-based hard zoning. When a device is zoned using both World-Wide Name (WWN) in one zone and <*domain, portarea*> in another, this will cause the port to go to session-based hard zoning.

In session-based zoning, the zone enforcement is checked by the software. In hardware-enforced zoning, zone or alias members are defined using <*domain, portarea*> exclusively or using WWNs exclusively: that is, using one method or the other to define all objects in the zoning database. If the devices on the port are defined by a mixture of port IDs and WWNs, the zone enforcement is session based. If the S_ID list of the hardware-enforced zoning overflows (over the S_ID limit), the hardware zone enforcement changes to session-based zoning.

Recommended Action No action is required.

Severity INFO

ZONE-1005

Message `<timestamp>, [ZONE-1005], <sequence-number>,, INFO, <system-name>, HARD &amp; SOFT zones(<Zone name>, <Zone name>) definitions overlap.`

Probable Cause Indicates a port is zoned with mixed devices (WWN and <*domain*, *portarea*>). During zoning database cross checking, it is detected that either:

- A port zone member is also listed as a member of a Mixed zone.
- A world-wide name (WWN) zone member is also specified as a member of a Mixed zone.

You should use hard zone enforcement whenever possible. Hard zones are more secure than "session-based hard zones". Both types of zones will trap a port login (PLOGI), but hard zones will filter out the I/O frames which **“session-based”** hard zones do not.

Recommended Action If hard zone enforcement is preferred, edit the zoning database to have the port zoned with devices defined as either WWN or defined as <*domain*, *portarea*>, but do not mix the methods used to define these zone members.

Severity INFO

ZONE-1006

Message `<timestamp>, [ZONE-1006], <sequence-number>,, WARNING, <system-name>, WARNING - WWN (<WWN number>)in HARD PORT zone <zone_name>.`

Probable Cause Indicates that one or more devices are zoned as world wide name (WWN) devices and also zoned as <*domain*, *portarea*> devices. The devices are used to specify zone members over separate zones.

Recommended Action If hardware zoning enforcement is preferred, edit the zoning database to have the device zoned using only one specification type, either WWN or <*domain*, *portarea*>.

Severity WARNING

ZONE-1007

Message `<timestamp>, [ZONE-1007], <sequence-number>,, INFO, <system-name>, Ioctl(<function>) in (<error message>) at port (<port number>) returns code (<error string>) and reason string (<reason string>).`

Probable Cause Indicates that frame filter logic reported a failure during one of the IOCTL calls. The IOCTL call from which the failure is reported is listed as part of the error message. This is usually a programming error when adding content-addressable memory (CAM) entries before the filter setup.

Recommended Action There are two ways to avoid this problem.

- Avoid having too many hosts zoned with a set of target devices at a single port.
- Avoid having too many zones directed at a single port group on the switch.

Severity INFO

ZONE-1008

Message `<timestamp>, [ZONE-1008], <sequence-number>,, WARNING, <system-name>, WARNING - port <port number> Out of CAM entries.`

Probable Cause Indicates the total number of entries of S_ID CAM is above the limit while creating or adding a zone group. The maximum number of content-addressable memory (CAM) entries allowed depends on the application-specific integrated circuit (ASIC).

Recommended Action If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

Severity WARNING

ZONE-1010

Message `<timestamp>, [ZONE-1010], <sequence-number>,, WARNING, <system-name>, WARNING - Duplicate entries in zone(<zone name>) specification.`

Probable Cause Indicates there are duplicate entries in a zone object. A zone object member is specified twice in a given zone object. This message occurs only when enabling a zone configuration.

Recommended Action Check the members of the zone and delete the duplicate member.

Severity WARNING

ZONE-1012

Message `<timestamp>, [ZONE-1012], <sequence-number>,, WARNING, <system-name>, WARNING - All ports are offline.`

Probable Cause Indicates that all the ports in a zone are offline.

Recommended Action Check the device connetion.

Severity WARNING

ZONE-1013

Message `<timestamp>, [ZONE-1013], <sequence-number>,, WARNING, <system-name>, Quick Loop not supported.`

Probable Cause Indicates the QuickLoop feature is not supported in the current code release. If the QuickLoop zoning configuration is enabled on the switch, it will not be supported.

Recommended Action Edit the zone database to remove the QuickLoop zoning definition in the effective configuration.

Severity WARNING

ZONE-1014

Message `<timestamp>, [ZONE-1014], <sequence-number>,, ERROR, <system-name>, Missing required license - <license name>.`

Probable Cause Indicates the required zoning license is missing.

Recommended Action Install the zoning license using the **licenseAdd** command. Refer to your switch supplier to obtain a zoning license if you do not have one.

Severity ERROR

ZONE-1015

Message `<timestamp>, [ZONE-1015], <sequence-number>,, WARNING, <system-name>, Not owner of the current transaction <transaction ID>.`

Probable Cause Indicates that a zoning change operation is not allowed because the zoning transaction is opened by another task. Indicates concurrent modification of the zone database by multiple administers.

Recommended Action Wait until the previous transaction is completed. Verify that only one administrator is working with the zone database at a time.

Severity WARNING

ZONE-1017

Message `<timestamp>, [ZONE-1017], <sequence-number>,, ERROR, <system-name>, FA Zone(<zone name>) contains incorrect number of Initiator and Target devices.`

Probable Cause Indicates the fabric assist (FA) zoning configuration has more than one initiator. The probable cause is incorrect entries in the FA zoning configuration.

Recommended Action Edit the zone database to ensure that only one initiator is set for each FA zone configuration.

Severity ERROR

ZONE-1018

Message `<timestamp>, [ZONE-1018], <sequence-number>,, ERROR, <system-name>, Incorrect zoning enforcement type(<zone type>) at port(<port number>).`

Probable Cause Indicates an incorrect zoning enforcement type was reported on the specified port. This is a software error. A QuickLoop zone type (value = 4) or an uninitialized type (value = 0) are invalid. The valid zone type values are:

- hard port zone (value = 1)
- hard wwn zone (value = 2)
- session based hard zoning (value = 3)
- FA zone (value = 5)

QuickLoop zones are not supported in Fabric OS v4.x and above.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

ZONE-1019

Message `<timestamp>, [ZONE-1019], <sequence-number>,, ERROR, <system-name>, Transaction Commit failed. Reason code <reason code> (<Application reason>) - \"<reason string>\"`

Probable Cause Indicates the reliable commit service (RCS) had a transmit error. RCS is a protocol used to transmit changes to the configuration database within a fabric.

Recommended Action Often this message indicates a transitory problem. Wait a few minutes and retry the command.

Make sure your changes to the zone database are not overwriting the work of another admin.

Run the **cfgTransShow** command to find out if there is any outstanding transaction running on the local switches.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

ZONE-1022

Message `<timestamp>, [ZONE-1022], <sequence-number>,, INFO, <system-name>, The effective configuration has changed to <Effective configuration name>. <AD Id>`

Probable Cause Indicates the effective zone configuration has changed to the name displayed.

Recommended Action Verify this zone configuration change was done on purpose. If the new effective zone configuration is correct, no action is necessary.

Severity INFO

ZONE-1023

Message `<timestamp>, [ZONE-1023], <sequence-number>,, INFO, <system-name>, Switch connected to port (<port number>) is busy. Retry zone merge.`

Probable Cause Indicates the switch is retrying the merge operation. This usually occurs if the switch on the other side of the port is busy.

Recommended Action If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

ZONE-1024

Message `<timestamp>, [ZONE-1024], <sequence-number>,, INFO, <system-name>, <Information message>.`

Probable Cause Indicates the **cfgSave** command ran successfully. The <*Information message*> is “cfgSave completes successfully.”

Recommended Action No action is required.

Severity INFO

ZONE-1026

Message `<timestamp>, [ZONE-1026], <sequence-number>,, INFO, <system-name>, port <port number> Out of CAM entries.`

Probable Cause Indicates the total number of S_ID entries while creating or adding a zone group exceeds the limit.

Recommended Action If hardware zoning enforcement is preferred, edit the zoning database to have zoned PIDs for that port.

Severity INFO

ZONE-1027

Message `<timestamp>, [ZONE-1027], <sequence-number>,, INFO, <system-name>, Zoning transaction aborted <error reason>. <AD Id>.`

Probable Cause Indicates the zoning transaction was aborted due to a variety of potential errors. The *error reason* variable can be one of the following:

- Zone Merge Received: The fabric is in the process of merging two zone databases.
- Zone Config update Received: The fabric is in the process of updating the zone database.
- Bad Zone Config: The new config is not viable.
- Zoning Operation failed: A zoning operation failed.
- Shell exited: The command shell has exited.
- Unknown: An error was received for an unknown reason.
- User Command: A user aborted the current zoning transaction.
- Switch Shutting Down: The switch is currently shutting down.

Recommended Action Many of the causes of this error message are transitory, for example, because two administrators are working with the zoning database concurrently. If you receive this error, wait for few minutes and try again. Ensure that no user is currently modifying the zone database.

Severity INFO

ZONE-1028

Message `<timestamp>, [ZONE-1028], <sequence-number>,, WARNING, <system-name>, Commit zone DB larger than supported - <zone db size> greater than <max zone db size>.`

Probable Cause Indicates the zone database size is greater than the limit allowed by the fabric. The limit of the zone database size depends on the lowest level switch in the fabric. Older switches have less memory and force a smaller zone database for the entire fabric.

Recommended Action Edit the zone database to keep it within the allowable limit for the specific switches in your fabric. Refer to the *Fabric OS Administrator's Guide* for information on the zone database sizes supported for each switch.

Severity WARNING

ZONE-1029

Message `<timestamp>, [ZONE-1029], <sequence-number>,, WARNING, <system-name>, Restoring zone cfg from flash failed - bad config saved to <config file name> [<return code>].`

Probable Cause Indicates the zone configuration restored from the flash was faulty.

Recommended Action This error will save the faulty zone configuration in the zoned core file directory.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity WARNING

ZONE-1030

Message `<timestamp>, [ZONE-1030], <sequence-number>,, WARNING, <system-name>, Converting the zone db for PID format change failed.`

Probable Cause Indicates the current zone database could not be converted to reflect the PID format change. Most likely this is caused by the size of the zone database.

Recommended Action Change the PID format back to its original format. Reduce the size of the zone database. Then you can change the PID format to the requested format.

Severity WARNING

ZONE-1031

Message `<timestamp>, [ZONE-1031], <sequence-number>,, ERROR, <system-name>, Switch is in interop mode. (switch, port) members not supported.`

Probable Cause Indicates the switch is set to interop mode using the **interopMode** command. Interop mode does not allow <*domain, portarea*> members in the active zone database.

Recommended Action Remove all <*domain, portarea*> members from the zone database, or convert them to world wide name (WWN) zoning.

Severity ERROR

ZONE-1032

Message `<timestamp>, [ZONE-1032], <sequence-number>,, ERROR, <system-name>, Domain <domain number> Max Zone DB size <max zone db size>.`

Probable Cause Indicates the specified domain does not have enough memory for the zone database being committed.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1033

Message `<timestamp>, [ZONE-1033], <sequence-number>,, ERROR, <system-name>, Domain <domain number> Lowest Max Zone DB size.`

Probable Cause Indicates the specified domain has the lowest memory available for the zone database in the fabric. The zone database must be smaller than the memory available on this domain.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1034

Message `<timestamp>, [ZONE-1034], <sequence-number>,, INFO, <system-name>, A new zone database file is created.`

Probable Cause Indicates that a new zone database was created.

Recommended Action No action is required.

Severity INFO

ZONE-1035

Message `<timestamp>, [ZONE-1035], <sequence-number>,, ERROR, <system-name>, Unable to rename <Old config file name> to <New config file name>: error message <System Error Message>.`

Probable Cause Indicates the Fabric OS cannot rename the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1036

Message `<timestamp>, [ZONE-1036], <sequence-number>,, ERROR, <system-name>, Unable to create <config file name>: error message <System Error Message>.`

Probable Cause Indicates the Fabric OS cannot create the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1037

Message `<timestamp>, [ZONE-1037], <sequence-number>,, ERROR, <system-name>, Unable to examine <config file name>: error message <System Error Message>.`

Probable Cause Indicates the Fabric OS cannot examine the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1038

Message `<timestamp>, [ZONE-1038], <sequence-number>,, ERROR, <system-name>, Unable to allocate memory for <config file name>: error message <System Error Message>.`

Probable Cause Indicates the Fabric OS cannot allocate enough memory for the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1039

Message `<timestamp>, [ZONE-1039], <sequence-number>,, ERROR, <system-name>, Unable to read contents of <config file name>: error message <System Error Message>.`

Probable Cause Indicates the Fabric OS cannot read the zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity ERROR

ZONE-1040

Message `<timestamp>, [ZONE-1040], <sequence-number>,, INFO, <system-name>, Merged zone database exceeds limit.`

Probable Cause Indicates the Fabric OS cannot read the merged zone configuration file. Typically the zone configuration is too large for the memory available on the switch.

Recommended Action Reduce the size of the zone database and retry the operation.

Severity INFO

ZONE-1041

Message `<timestamp>, [ZONE-1041], <sequence-number>,, WARNING, <system-name>, Unstable link detected during merge at port (<Port number>).`

Probable Cause Indicates a possible unstable link or faulty cable.

Recommended Action Check the SFP and cable at the specified port and verify that they are not faulty. Replace the SFP and cable as necessary.

Severity WARNING

ZONE-1042

Message `<timestamp>, [ZONE-1042], <sequence-number>,, INFO, <system-name>, The effective configuration has been disabled. <AD Id>.`

Probable Cause Indicates the effective zone configuration has been disabled.

Recommended Action Verify that this zone configuration change was done on purpose. If no effective zone configuration is needed, no action is necessary.

Severity INFO

ZONE-1043

Message `<timestamp>, [ZONE-1043], <sequence-number>,, INFO, <system-name>, The Default Zone access mode is set to No Access.`

Probable Cause Indicates the Default Zone access mode is set to No Access.

Recommended Action Verify that this Default Zone access mode change was done intentionally.

Severity INFO

ZONE-1044

Message `<timestamp>, [ZONE-1044], <sequence-number>,, INFO, <system-name>, The Default Zone access mode is set to All Access.`

Probable Cause Indicates that the Default Zone access mode is set to All Access.

Recommended Action Verify that this Default Zone access mode change was done intentionally.

Severity INFO

ZONE-1045

Message `<timestamp>, [ZONE-1045], <sequence-number>,, INFO, <system-name>, The Default Zone access mode is already set to No Access.`

Probable Cause Indicates that the Default Zone access mode is already set to No Access.

Recommended Action No action is required.

Severity INFO

ZONE-1046

Message `<timestamp>, [ZONE-1046], <sequence-number>,, INFO, <system-name>, The Default Zone access mode is already set to All Access.`

Probable Cause Indicates the Default Zone access mode is already set to All Access.

Recommended Action No action is required.

Severity INFO

ZONE-1047

Message `<timestamp>, [ZONE-1047], <sequence-number>,, INFO, <system-name>, Switch domain (<domainr>) does not support defined database.`

Probable Cause Indicates a remote Brocade switch is running a downlevel version of Fabric OS that does not support the defined database.

Recommended Action It is recommended to upgrade all switches to the same release level version.

Severity INFO

ZONE-1048

Message `<timestamp>, [ZONE-1048], <sequence-number>,, WARNING, <system-name>, SZONE ACA is rejected on the standby.`

Probable Cause Indicates that the standby zoning component has not received a **syncdump** command from the primary side.

Recommended Action Synchronize the standby CP.

Severity WARNING

ZONE-1049

Message `<timestamp>, [ZONE-1049], <sequence-number>,, ERROR, <system-name>, ZONE AD-DefZone conflict detected while system initialization.`

Probable Cause Indicates that there is an AD-DefZone conflict.

Recommended Action Check and resolve the default zone mismatch issue.

Severity ERROR

ZONE-1050

Message `<timestamp>, [ZONE-1050], <sequence-number>,, INFO, <system-name>, The Interop Safe Zoning mode is set to Enabled.`

Probable Cause Indicates that the Interop Safe Zoning mode is enabled.

Recommended Action Verify if the Safe Zoning mode change was done on purpose.

Severity INFO

ZONE-1051

Message `<timestamp>, [ZONE-1051], <sequence-number>,, INFO, <system-name>, The Interop Safe Zoning mode is set to Disabled.`

Probable Cause Indicates that the Interop Safe Zoning mode is disabled.

Recommended Action Verify if the Safe Zoning mode change was done on purpose.

Severity INFO

ZONE-1052

Message `<timestamp>, [ZONE-1052], <sequence-number>,, INFO, <system-name>, The Interop Default Zone state is set to enabled.`

Probable Cause Indicates the Interop Default Zone attribute state is enabled.

Recommended Action Verify if the Interop Default Zone attribute state change was done on purpose.

Severity INFO

ZONE-1053

Message `<timestamp>, [ZONE-1053], <sequence-number>,, INFO, <system-name>, The Default Zone state is set to Disabled.`

Probable Cause Indicates the Interop Default Zone attribute state is disabled.

Recommended Action Verify if the Interop Default Zone attribute state change was done on purpose.

Severity INFO

ZONE-1054

Message `<timestamp>, [ZONE-1054], <sequence-number>,, WARNING, <system-name>, DEFZONE ALLACCESS set with Frame Redirection zones.`

Probable Cause Indicates the DEFZONE allaccess mode will not grant all access behavior when frame redirection zones are defined.

Recommended Action Remove frame redirection zones or set the **defzone** command to noaccess mode.

Severity WARNING

ZONE-1055

Message `<timestamp>, [ZONE-1055], <sequence-number>,, WARNING, <system-name>, McDATA default zone enabled with Frame Redirection zones.`

Probable Cause Indicates that frame redirection will not function properly with McDATA default zoning.

Recommended Action Remove frame redirection zones or disable McDATA default zoning.

Severity WARNING

ZONE-1056

Message `<timestamp>, [ZONE-1056], <sequence-number>,, WARNING, <system-name>, Non-ETIZ-Capable Switch (dom <domain id>) in fabric w/ETIZ Configured.`

Probable Cause Indicates the config Save/Enable/Disable operations will not work with pre-6.4.0 FOS switch in IM2 fabric when ETIZ Zones are configured.

Recommended Action Remove pre-6.4.0 FOS switch from fabric or delete Enhanced TI Zone(s).

Severity WARNING

ZONE-1057

Message `<timestamp>, [ZONE-1057], <sequence-number>,, WARNING, <system-name>, TI Zone <TI zone name> has domain <Domain ID of switch with version pre6.4.0> running pre FOS6.4.0 firmware. TI member (Domain <Domain ID of higher port index>, Index <Higher port index>) is not supported.`

Probable Cause Indicates that an unsupported port index(> 511) is present in the TI zone path.

Recommended Action Remove the port index from the TI zone or the routing may not be setup correctly.

Severity WARNING

Section

II

Audit Log Messages

This section provides the Audit messages, including:

Chapter

AUDIT AG System Messages

112

AG-1033

Message `AUDIT, <timestamp>, [AG-1033], <sequence-number>,, INFO, <system-name>,F_Port to N_Port mapping has been updated for N_Port (<n_port>) .`

Probable Cause Indicates that the F_Ports mapped to an N_Port have changed and the configuration file has been updated.

Recommended Action No action is required.

Severity INFO

AG-1034

Message `AUDIT, <timestamp>, [AG-1034], <sequence-number>,, INFO, <system-name>,F_Port cannot accept any more logins (<fport>) .`

Probable Cause Indicates that the F_Port has already logged in the maximum number of devices.

Recommended Action No action is required.

Severity INFO

AG-1035

Message `AUDIT, <timestamp>, [AG-1035], <sequence-number>,, INFO, <system-name>,Device cannot login as ALPA value not available (<alpa>) .`

Probable Cause Indicates that a device has already used this ALPA value.

Recommended Action No action is required.

Severity INFO

AG-1036

Message `AUDIT, <timestamp>, [AG-1036], <sequence-number>,, WARNING, <system-name>,Port <port> is connected to a Non-Brocade fabric with Persistent ALPA enabled. Check the admin guide for supported configuration .`

Probable Cause Indicates that one of the ports is connected to a Non-Brocade Fabric.

Recommended Action No action is required.

Severity WARNING

AG-1037

Message

```
AUDIT, <timestamp>, [AG-1037], <sequence-number>,, INFO, <system-name>,Trunked
N_Port (<nport>) going offline, if switchshow CLI for the connected fabric switch
port displays Persistently disabled: Area has been acquired, then check cabling:
all trunked ports should be in same ASIC Port Group .
```

Probable Cause Indicates that the cabling is incorrect.

Recommended Action If the **switchshow** command on the connected fabric switch port displays 'Persistently disabled: Area has been acquired', then check the cabling on the AG. All trunked ports in a single trunk should belong to the same ASIC Port Group.

Severity INFO

Chapter

AUDIT AN System Messages

113

AN-1003

Message `<timestamp>, [AN-1003], <sequence-number>,, WARNING, <system-name>, Slot <slot number>, port <port number within slot number> is a latency bottleneck. <percentage of seconds affected by latency bottlenecking> percent of last <observation period over which the percentage of affected seconds is reported> seconds were affected by this condition.`

Probable Cause For an F_Port, it indicates that the attached device is slow in responding to frames going out of this port. This latency may be inherent in the device or due to heavy workload on the device. For an E_Port, it indicates a downstream primary bottleneck.

Recommended Action Find the Top Talkers in the egress direction from this port and apply Ingress Rate Limiting to one or more of them.

Severity WARNING

AN-1004

Message `<timestamp>, [AN-1004], <sequence-number>,, WARNING, <system-name>, Slot <slot number>, port <port number within slot number> is a congestion bottleneck. <percentage of seconds affected by congestion bottlenecking> percent of last <observation period over which the percentage of affected seconds is reported> seconds were affected by this condition.`

Probable Cause Indicates that the volume of outgoing traffic at this port is too high for the capacity of the link.

Recommended Action Add more capacity on the path, using trunk links if possible.

Severity WARNING

AN-1005

Message `<timestamp>, [AN-1005], <sequence-number>,, WARNING, <system-name>, Slot <slot number>, port <port number within slot number> has <bottleneck type> bottleneck cleared.`

Probable Cause Indicates that the bottleneck was cleared on the port.

Recommended Action No action is required.

Severity WARNING

AN-1006

Message `<timestamp>, [AN-1006], <sequence-number>,, INFO, <system-name>, Bottleneck detection configuration is successfully changed.`

Probable Cause Indicates that the bottleneck detection configuration was changed by a user.

Recommended Action No action is required.

Severity INFO

AN-1010

Message `<timestamp>, [AN-1010], <sequence-number>,, WARNING, <system-name>, Severe latency bottleneck detected at Slot <slot number> port <port number within slot number>.`

Probable Cause Indicates a credit loss.

Recommended Action Contact your vendor's customer support for assistance.

Severity WARNING

Chapter

AUDIT AUTH System Messages

114

AUTH-1045

Message `AUDIT, <timestamp>, [AUTH-1045], <sequence-number>,, ERROR, <system-name>, Certificate not present in this switch in <authentication phase> port <port number>.`

Probable Cause Indicates that the public key infrastructure (PKI) certificate is not installed in this switch.

Recommended Action Check the certificate availability using the **pkiShow** command. Install the certificate and reinitialize authentication using the **portDisable** and **portEnable** commands or the **switchDisable** and **switchEnable** commands.

If the message persists, run **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-1046

Message `AUDIT, <timestamp>, [AUTH-1046], <sequence-number>,, INFO, <system-name>, <Operation type> has been successfully completed.`

Probable Cause Indicates that the certificate database operation has been updated using the **secAuthCertificate** command. The values for Operation type can be "set" or "remove".

Recommended Action No action is required.

Severity INFO

AUTH-1047

Message `AUDIT, <timestamp>, [AUTH-1047], <sequence-number>,, ERROR, <system-name>, <Operation type> has failed.`

Probable Cause Indicates that the specified action has failed to update the certificate database using the **secAuthCertificate** command. The values for Operation type can be "set" or "remove".

Recommended Action Retry the **secAuthCertificate** command.

Run supportFtp (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity ERROR

AUTH-3001

Message `AUDIT, <timestamp>, [AUTH-3001], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <Data type> type has been changed from [<Old value>] to [<New value>].`

Probable Cause Indicates that an authentication configuration value was set to a specified value. The *data type* can be either “authentication type”, “DH group type”, “Hash type” or “policy type”.

Recommended Action No action is required.

Severity INFO

AUTH-3002

Message `AUDIT, <timestamp>, [AUTH-3002], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <Event Related Info>.`

Probable Cause Indicates that the secret database operation has been updated using the **secAuthSecret** command.

Recommended Action No action is required.

Severity INFO

AUTH-3003

Message `AUDIT, <timestamp>, [AUTH-3003], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <Operation type> the PKI objects.`

Probable Cause Indicates that the public key infrastructure (PKI) objects were created using the **pkiCreate** command or that the PKI objects were removed using the **pkiRemove** command. The *Operation Type* can be either “Created” or “Removed”.

Recommended Action No action is required.

Severity INFO

AUTH-3004

Message `AUDIT, <timestamp>, [AUTH-3004], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: failed, Info: Neighboring switch has a conflicting authentication policy; Port <Port Number> disabled.`

Probable Cause The specified E_Port was disabled because the neighboring switch rejected the authentication negotiation, and the local switch has a strict switch authentication policy.

Recommended Action Correct the switch policy configuration on either of the switches using the **authUtil** command, and then enable the specified port using the **portEnable** command.

Severity INFO

AUTH-3005

Message

```
AUDIT, <timestamp>, [AUTH-3005], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: failed, Info: Rejecting
authentication request on port <Port Number> because switch policy is turned off.
```

Probable Cause Indicates that the local switch has rejected the authentication request, because the switch policy is turned off. If the neighboring switch has a strict (ON) switch policy, the light will go off due to conflicting configuration settings. Otherwise the E_Port will form without authentication.

Recommended Action If the light on the specified port is off, correct the switch policy configuration on either of the switches using **the authUtil** command, and then enable the port on the neighboring switch using the **portEnable** command. If the E_Port formed no action is required.

Severity INFO

AUTH-3006

Message

```
AUDIT, <timestamp>, [AUTH-3006], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: failed, Info: Authentication
failed on port <port number> due to mismatch of DH-CHAP shared secrets.
```

Probable Cause Indicates that an authentication operation using a Diffie Hellman - challenge-handshake authentication protocol (DH-CHAP) failed on the specified port due to mismatched response values between two entities.

The error might indicate that an invalid entity attempted to connect to the switch.

Recommended Action Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

AUTH-3007

Message

```
AUDIT, <timestamp>, [AUTH-3007], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: failed, Info: Port <port number>
disabled due to receiving an authentication reject with code '<Reason String>' and
explanation '<Explanation String>'.
```

Probable Cause Indicates that the specified port was disabled due to receiving an authentication reject response from the connected switch/device.

The error might indicate that an invalid entity attempted to connect to the switch.

Recommended Action Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run **supportFtp** (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

AUTH-3008

Message

```
AUDIT, <timestamp>, [AUTH-3008], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: failed, Info: Port <port number>
has been disabled due to authentication failure with code '<Reason String>' and
explanation '<Explanation String>'.
```

Probable Cause Indicates that the specified port has been disabled, because the connecting switch/device failed to authenticate.

The error might indicate that an invalid entity attempted to connect to the switch.

Recommended Action Check the connection port for a possible security attack.

Check the shared secrets using the **secAuthSecret** command and reinitialize authentication using the **portDisable** and **portEnable** commands.

If the message persists, run the **supportFtp** command (as needed) to set up automatic FTP transfers; then run the **supportSave** command and contact your switch service provider.

Severity INFO

Chapter

AUDIT BLS System Messages

115

BLS-1002

Message `<timestamp>, [BLS-1002], <sequence-number>,, INFO, <system-name>, An IPsec/IKE policy was added.`

Probable Cause Indicates that an IPsec or IKE policy was added and the configuration file was updated.

Recommended Action No action is required.

Severity INFO

BLS-1003

Message `<timestamp>, [BLS-1003], <sequence-number>,, INFO, <system-name>, An IPsec/IKE policy was deleted.`

Probable Cause Indicates that an IPsec or IKE policy was deleted and the configuration file was updated.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT CNM System Messages

116

CNM-3001

Message `AUDIT, <timestamp>, [CNM-3001], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: encryption group \<encryptiongroupname>\ created.`

Probable Cause Indicates an encryption group was created.

Recommended Action No action is required.

Severity INFO

CNM-3002

Message `AUDIT, <timestamp>, [CNM-3002], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: encryption group deleted.`

Probable Cause Indicates an encryption group was deleted.

Recommended Action No action is required.

Severity INFO

CNM-3003

Message `AUDIT, <timestamp>, [CNM-3003], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Membernode \<membernodeWWN>\ added to encryption group.`

Probable Cause Indicates a membernode was added to an encryption group.

Recommended Action No action is required.

Severity INFO

CNM-3004

Message `AUDIT, <timestamp>, [CNM-3004], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Membernode \<membernodeWWN>\ ejected from encryption group.`

Probable Cause Indicates a membernode was ejected from an encryption group.

Recommended Action No action is required.

Severity INFO

CNM-3005

Message `AUDIT, <timestamp>, [CNM-3005], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Membernode \<membernodeWWN>\ left encryption group.`

Probable Cause Indicates the membernode left an encryption group.

Recommended Action No action is required.

Severity INFO

CNM-3006

Message `AUDIT, <timestamp>, [CNM-3006], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Heartbeat miss count set to <hbmisses>.`

Probable Cause Indicates that the heartbeat miss value was set.

Recommended Action No action is required.

Severity INFO

CNM-3007

Message `AUDIT, <timestamp>, [CNM-3007], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Heartbeat timeout set to <hbtimeout>.`

Probable Cause Indicates that the heartbeat timeout value was set.

Recommended Action No action is required.

Severity INFO

CNM-3008

Message `AUDIT, <timestamp>, [CNM-3008], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Routing mode of EE in slot <slot> set to <routingmode>.`

Probable Cause Indicates that the encryption engine (EE) routing mode was set.

Recommended Action No action is required.

Severity INFO

CNM-3009

Message `AUDIT, <timestamp>, [CNM-3009], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Membernode <membernodeWWN> registered.`

Probable Cause Indicates a membernode was registered.

Recommended Action No action is required.

Severity INFO

CNM-3010

Message `AUDIT, <timestamp>, [CNM-3010], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Membernode <membernodeWWN> unregistered.`

Probable Cause Indicates a membernode was unregistered.

Recommended Action No action is required.

Severity INFO

CNM-3011

Message `AUDIT, <timestamp>, [CNM-3011], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Encryption group synchronized.`

Probable Cause Indicates an encryption group was synchronized.

Recommended Action No action is required.

Severity INFO

CNM-3012

Message `AUDIT, <timestamp>, [CNM-3012], <sequence-number>,, INFO, <system-name>, Deleteing an EG with luns setup for encryption can lead to luns being disabled if Encryption Group name is not preserved (<egname>).`

Probable Cause Indicates that the Encryption Group (EG) was deleted, recreate EG with the same name if luns are setup for encryption.

Recommended Action Preserve EG name when EG is recreated if luns are setup for encryption.

Severity INFO

Chapter

AUDIT CONF System Messages

117

CONF-1000

Message `AUDIT, <timestamp>, [CONF-1000], INFO, CFG, <event-initiator-details>, <event-location>, , configDownload completed successfully. <Info about the parameters and AD>.`

Probable Cause Indicates that the **configDownload** operation was initiated and completed successfully. The statement that follows, message string, is the description of the classes of configuration parameters that were downloaded. If Admin Domain (AD) is enabled, the AD number is specified in the description.

Recommended Action No action is required.

Severity INFO

CONF-1001

Message `AUDIT, <timestamp>, [CONF-1001], INFO, CFG, <event-initiator-details>, <event-location>, , configDownload completed successfully. <Info about the parameters and AD>.`

Probable Cause Indicates that the **configDownload** process was initiated and completed successfully. The statement that follows, message string, is the description of the classes of configuration parameters that were downloaded. If Admin Domain (AD) is enabled, the AD number is specified in the description.

Recommended Action No action is required.

Severity INFO

CONF-1020

Message `AUDIT, <timestamp>, [CONF-1020], INFO, CFG, <event-initiator-details>, <event-location>, , configDownload not permitted <AD Number if AD is configured on the system>.`

Probable Cause Indicates a **configDownload** operation is not permitted. There are several possible causes.

Recommended Action Check the error log, correct the error and rerun the **configDownload** command.

Severity INFO

CONF-1022

Message `AUDIT, <timestamp>, [CONF-1022], WARNING, CFG, <event-initiator-details>, <event-location>, , Downloading configuration without disabling the switch was unsuccessful.`

Probable Cause Indicates an attempt to download the configuration without disabling the switch was unsuccessful because there are one or more parameters that require the switch to be disabled.

Recommended Action Disable the switch using the **switchDisable** command and download the configuration.

Severity WARNING

CONF-1042

Message `<timestamp>, [CONF-1042], <sequence-number>,, INFO, <system-name>, Fabric Configuration Parameter <parameter> changed to <value>.`

Probable Cause Indicates that the parameter value has been changed.

Recommended Action No action is required.

Severity INFO

CONF-1043

Message `<timestamp>, [CONF-1043], <sequence-number>,, INFO, <system-name>, Fabric Configuration Parameter <parameter> changed to <value>.`

Probable Cause Indicates that the parameter value has been changed.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT CVLM System Messages

118

CVLM-3001

Message `AUDIT, <timestamp>, [CVLM-3001], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Failback mode set to <failbackmode>.`

Probable Cause Indicates that the failback mode was set.

Recommended Action No action is required.

Severity INFO

CVLM-3002

Message `AUDIT, <timestamp>, [CVLM-3002], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: HA cluster <HAClusterName> created.`

Probable Cause Indicates an HA cluster was created.

Recommended Action No action is required.

Severity INFO

CVLM-3003

Message `AUDIT, <timestamp>, [CVLM-3003], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: HA cluster <HAClusterName> deleted.`

Probable Cause Indicates a HA cluster was deleted.

Recommended Action No action is required.

Severity INFO

CVLM-3004

Message `AUDIT, <timestamp>, [CVLM-3004], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Cluster member added to HA cluster <HAClusterName>.`

Probable Cause Indicates a HA cluster member was added to an HA cluster.

Recommended Action No action is required.

Severity INFO

CVLM-3005

Message `AUDIT, <timestamp>, [CVLM-3005], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Cluster member removed from HA cluster <HAClusterName>.`

Probable Cause Indicates a HA cluster member was removed from an HA cluster.

Recommended Action No action is required.

Severity INFO

CVLM-3006

Message `AUDIT, <timestamp>, [CVLM-3006], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Current node WWN/slot <CurrentWWN> / <CurrentSlot> replaced with new node WWN/slot: <NewWWN> / <NewSlot>.`

Probable Cause Indicates a HA cluster member was replaced.

Recommended Action No action is required.

Severity INFO

CVLM-3007

Message `AUDIT, <timestamp>, [CVLM-3007], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: <diskOrTape> container \<containerName>\ created.`

Probable Cause Indicates a cryptotarget container was created.

Recommended Action No action is required.

Severity INFO

CVLM-3008

Message `AUDIT, <timestamp>, [CVLM-3008], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Container \<containerName>\ deleted.`

Probable Cause Indicates a cryptotarget container was deleted.

Recommended Action No action is required.

Severity INFO

CVLM-3009

Message `AUDIT, <timestamp>, [CVLM-3009], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Manual failback from EE <currentnodeWWN>/<currentSlot> to EE <newnodeWWN>/<newnodeSlot>.`

Probable Cause Indicates a manual failback was performed to an encryption engine.

Recommended Action No action is required.

Severity INFO

CVLM-3010

Message `AUDIT, <timestamp>, [CVLM-3010], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Move crypto container \<cryptoTargetContainer>\ to EE <newEEWWN>/<newEESlot>.`

Probable Cause Indicates a cryptotarget container was moved to another encryption engine.

Recommended Action No action is required.

Severity INFO

CVLM-3011

Message `AUDIT, <timestamp>, [CVLM-3011], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Initiator PWWN \<initiatorPWWN>\ Initiator NWWN \<initiatorNWWN>\ added to crypto target container \<cryptoTargetContainer>\.`

Probable Cause Indicates an initiator was added to a cryptotarget container.

Recommended Action No action is required.

Severity INFO

CVLM-3012

Message

```
AUDIT, <timestamp>, [CVLM-3012], INFO, , <event-initiator-details>,
<event-location>, , Event: cryptocfg Status: success, Info: Initiator
\<initiator>\ removed from crypto target container \<cryptoTargetContainer>\.
```

Probable Cause Indicates an initiator was removed from a cryptotarget container.

Recommended Action No action is required.

Severity INFO

CVLM-3013

Message

```
AUDIT, <timestamp>, [CVLM-3013], INFO, , <event-initiator-details>,
<event-location>, , Event: cryptocfg Status: success, Info: LUN <LUNSpec>,
attached through Initiator \<Initiator>\, added to crypto target container
\<cryptoTargetContainer>\.
```

Probable Cause Indicates a LUN was added to a cryptotarget container.

Recommended Action No action is required.

Severity INFO

CVLM-3014

Message

```
AUDIT, <timestamp>, [CVLM-3014], INFO, , <event-initiator-details>,
<event-location>, , Event: cryptocfg Status: success, Info: Lun <LUNNumber>,
attached through Initiator \<Initiator>\, in crypto target container
\<cryptoTargetContainer>\ modified.
```

Probable Cause Indicates a LUN in a cryptotarget container was modified.

Recommended Action No action is required.

Severity INFO

CVLM-3015

Message `AUDIT, <timestamp>, [CVLM-3015], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Lun <LUNNumber>, attached through Initiator \<Initiator>\, removed from crypto target container \<cryptoTargetContainer>\.`

Probable Cause Indicates a LUN was removed from a cryptotarget container.

Recommended Action No action is required.

Severity INFO

CVLM-3016

Message `AUDIT, <timestamp>, [CVLM-3016], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Lun <LUNNumber>, attached through Initiator \<Initiator>\, in crypto target container \<cryptoTargetContainer>\ enabled.`

Probable Cause Indicates a LUN in a cryptotarget container was enabled.

Recommended Action No action is required.

Severity INFO

CVLM-3017

Message `AUDIT, <timestamp>, [CVLM-3017], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Tape pool \<tapepoolLabelOrNum>\ created.`

Probable Cause Indicates a tapepool was created.

Recommended Action No action is required.

Severity INFO

CVLM-3018

Message `AUDIT, <timestamp>, [CVLM-3018], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Tape pool \<tapepoolLabelOrNum>\ deleted.`

Probable Cause Indicates a tapepool was deleted.

Recommended Action No action is required.

Severity INFO

CVLM-3019

Message
```
AUDIT, <timestamp>, [CVLM-3019], INFO, , <event-initiator-details>,
<event-location>, , Event: cryptocfg Status: success, Info: Tape pool
\<tapepoolLabelOrNum>\ modified.
```

Probable Cause Indicates a tapepool was modified.

Recommended Action No action is required.

Severity INFO

CVLM-3020

Message
```
AUDIT, <timestamp>, [CVLM-3020], INFO, , <event-initiator-details>,
<event-location>, , Event: cryptocfg Status: success, Info: Manual rekey of LUN
<LUNSpec> attached through Initiator \<Initiator>\ in crypto tgt container
\<cryptoTargetContainer>\.
```

Probable Cause Indicates a manual rekey of a LUN was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3021

Message
```
AUDIT, <timestamp>, [CVLM-3021], INFO, , <event-initiator-details>,
<event-location>, , Event: cryptocfg Status: success, Info: Manual rekey all
performed.
```

Probable Cause Indicates a complete manual rekey was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3022

Message `AUDIT, <timestamp>, [CVLM-3022], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Resume rekey of LUN <LIUNSpec> attached through Initiator \<Initiator>\ in crypto tgt container \<cryptoTargetContainer>\.`

Probable Cause Indicates a resume rekey was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3023

Message `AUDIT, <timestamp>, [CVLM-3023], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Transaction committed.`

Probable Cause Indicates a transaction commit operation was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3024

Message `AUDIT, <timestamp>, [CVLM-3024], INFO, , <event-initiator-details>, <event-location>, , Event: cryptocfg Status: success, Info: Transaction <transactionID> aborted.`

Probable Cause Indicates a transaction abort operation was performed.

Recommended Action No action is required.

Severity INFO

CVLM-3025

Message `AUDIT, <timestamp>, [CVLM-3025], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: started, Info: Decommission of device (container <cryptoTargetContainer> initiator <Initiator>, LUN <Lun>).`

Probable Cause Indicates that the decommission operation has started.

Recommended Action No action is required.

Severity INFO

CVLM-3026

Message `AUDIT, <timestamp>, [CVLM-3026], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: failed, Info: Decommission of device (container <cryptoTargetContainer> initiator <Initiator>, LUN <Lun>).`

Probable Cause Indicates that the decommission operation has failed for the device.

Recommended Action Reissue the decommission command.

Severity INFO

CVLM-3027

Message `AUDIT, <timestamp>, [CVLM-3027], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: Decommission of device (container <cryptoTargetContainer> initiator <Initiator>, LUN <Lun>).`

Probable Cause Indicates that the decommission operation has been completed for the device.

Recommended Action No action is required.

Severity INFO

CVLM-3028

Message `AUDIT, <timestamp>, [CVLM-3028], <sequence-number>,, INFO, <system-name>, Event: cryptocfg Status: success, Info: SRDF mode set to <srdfmode>.`

Probable Cause Indicates that the SRDF mode was set.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT FCIP System Messages

119

FCIP-1002

Message `AUDIT, <timestamp>, [FCIP-1002], INFO, CFG, <event-initiator-details>, <event-location>, , An IPsec/IKE policy was added.`

Probable Cause Indicates that an IPsec/IKE policy was added and the config file was updated.

Recommended Action No action is required.

Severity INFO

FCIP-1003

Message `AUDIT, <timestamp>, [FCIP-1003], INFO, CFG, <event-initiator-details>, <event-location>, , An IPsec/IKE policy was deleted.`

Probable Cause Indicates that an IPsec/IKE policy was deleted and the config file was updated.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT FICU System Messages

120

FICU-1011

Message `AUDIT, <timestamp>, [FICU-1011], INFO, CFG, <event-initiator-details>, <event-location>, , FMS mode has been enabled.`

Probable Cause Indicates that the FICON Management server mode has been enabled.

Recommended Action No action is required.

Severity INFO

FICU-1012

Message `AUDIT, <timestamp>, [FICU-1012], INFO, CFG, <event-initiator-details>, <event-location>, , FMS mode has been disabled.`

Probable Cause Indicates that the FICON Management server mode has been disabled.

Recommended Action No action is required.

Severity INFO

FICU-1019

Message `AUDIT, <timestamp>, [FICU-1019], <sequence-number>,, INFO, <system-name>, Switch has been set offline by LP(%s).`

Probable Cause Indicates the Fibre Connectivity (FICON) Management server has disabled switch.

Recommended Action No action is required.

Severity INFO

FICU-1020

Message `AUDIT, <timestamp>, [FICU-1020], <sequence-number>,, INFO, <system-name>, Port Addrs (%s) have been Blocked by %s.`

Probable Cause Indicates the Fibre Connectivity (FICON) Management server has blocked ports.

Recommended Action No action is required.

Severity INFO

FICU-1021

Message `AUDIT, <timestamp>, [FICU-1021], <sequence-number>,, INFO, <system-name>, Port Addrs (%s) have been UnBlocked by %s.`

Probable Cause Indicates the Fibre Connectivity (FICON) Management server has unblocked ports.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT FW System Messages

121

FW-3001

Message `AUDIT, <timestamp>, [FW-3001], INFO, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info:<Event Related info>`

Probable Cause Indicates that Port Fencing was enabled/disabled successfully.

Recommended Action No action is required.

Severity INFO

121 FW-3001

Chapter

AUDIT HTTP System Messages

122

HTTP-1002

Message `AUDIT, <timestamp>, [HTTP-1002], INFO, ZONE, <event-initiator-details>, <event-location>, , Zoning transaction initiated by User: <User Name>, Role: <User Role> completed successfully.`

Probable Cause Indicates that the zoning database has been changed.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

HTTP-1003

Message `AUDIT, <timestamp>, [HTTP-1003], INFO, ZONE, <event-initiator-details>, <event-location>, , Zoning transaction initiated by User: <User Name>, Role: <User Role> could not be completed successfully - <Reason Message>.`

Probable Cause Indicates an error occurred while completing the zoning transaction.

Recommended Action Verify that the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

Chapter

AUDIT IPAD System Messages

123

IPAD-1002

Message `AUDIT, <timestamp>, [IPAD-1002], INFO, CFG, <event-initiator-details>, <event-location>, , Switchname has been successfully changed to <Switch name>.`

Probable Cause Indicates that a change with the switch name has occured.

Recommended Action No action is required.

Severity INFO

123 IPAD-1002

Chapter

AUDIT PORT System Messages

124

PORT-1006

Message `AUDIT, <timestamp>, [PORT-1006], INFO, CFG, <event-initiator-details>, <event-location>, , Configuration changed for port (ID: <port number>) in No_Module or No_Light state.`

Probable Cause Indicates the configuration changes were made to an offline port in No_Module or No_Light state.

Recommended Action No action is required.

Severity INFO

PORT-1007

Message `AUDIT, <timestamp>, [PORT-1007], INFO, CFG, <event-initiator-details>, <event-location>, , Port (ID: <port number>) has been renamed to <port name>.`

Probable Cause Indicates a port has been reconfigured with a different name.

Recommended Action No action is required.

Severity INFO

PORT-1008

Message `AUDIT, <timestamp>, [PORT-1008], INFO, CFG, <event-initiator-details>, <event-location>, , GigE Port (ID: <port number>) has been enabled.`

Probable Cause Indicates a GigE port has been enabled.

Recommended Action No action is required.

Severity INFO

PORT-1009

Message `AUDIT, <timestamp>, [PORT-1009], INFO, CFG, <event-initiator-details>, <event-location>, , GigE Port (ID: <port number>) has been disabled.`

Probable Cause Indicates a GigE port has been disabled.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT SEC System Messages

125

SEC-1113

Message `<timestamp>, [SEC-1113], <sequence-number>,, WARNING, <system-name>, <Key> [ <Feature> license ] going to expire in <Expiry_days> days.`

Probable Cause Indicates the license period will expire soon.

Recommended Action Get a new license for this feature.

Severity WARNING

SEC-1114

Message `<timestamp>, [SEC-1114], <sequence-number>,, WARNING, <system-name>, <Key> [ <Feature> license ] is expired.`

Probable Cause Indicates the license period has expired.

Recommended Action Get a new license for this feature.

Severity WARNING

SEC-3001

Message `AUDIT, <timestamp>, [SEC-3001], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Security mode <State change: Enabled or Disabled> on the fabric.`

Probable Cause Indicates the security mode of the fabric was either enabled or disabled.

Recommended Action Verify the security mode change was planned. If the security mode change was planned, no action is required. If the security mode change was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3002

Message `AUDIT, <timestamp>, [SEC-3002], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <Event Related Info>.`

Probable Cause Indicates the specified security event has occurred. The *Event Name* can be one of the following:

- There has been an fabric configurations server (FCS) failover.
- A security policy has been activated.
- A security policy has been saved.
- A security policy has been aborted.
- A non-FCS password has changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3003

Message `AUDIT, <timestamp>, [SEC-3003], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Created <Policy Name> policy, with members <Member List> .`

Probable Cause Indicates a new security policy was created with entries.
Note: If you use a wildcard (for example, an asterisk) in creating a policy, the audit report displays the wildcard in the event info field.

Recommended Action Verify the new policy creation was planned. If the new policy creation was planned, no action is required. If the new policy creation was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3004

Message `AUDIT, <timestamp>, [SEC-3004], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Created <Policy name> policy.`

Probable Cause Indicates a new security policy was created.
Note: If you use a wildcard (for example, an asterisk) in creating a member for a policy, the audit message displays the wildcard in the event info field.

Recommended Action Verify the new policy creation was planned. If the new policy creation was planned, no action is required. If the new policy creation was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3005

Message `AUDIT, <timestamp>, [SEC-3005], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Added members <Members added> to policy <Policy name>.`

Probable Cause Indicates new members have been added to the specified security policy.
Note: If you use a wildcard (for example, an asterisk) in adding members to a policy, the audit report displays the wildcard in the event info field.

Recommended Action Verify the addition of members to the policy was planned. If the addition of members was planned, no action is required. If the addition of members was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3006

Message `AUDIT, <timestamp>, [SEC-3006], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Removed members <Members removed> from policy <Policy name>.`

Probable Cause Indicates a user has removed the specific members from the specified security policy.
Note: If you use a wildcard (for example, an asterisk) in removing members from a policy, the audit report displays the wildcard in the event info field.

Recommended Action Verify the removal of members to the policy was planned. If the removal of members was planned, no action is required. If the removal of members was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3007

Message `AUDIT, <timestamp>, [SEC-3007], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Deleted policy <Deleted policy name>.`

Probable Cause Indicates the specified security policy was deleted.

Recommended Action Verify the policy deletion was planned. If the policy deletion was planned, no action is required. If the policy deletion was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3008

Message `AUDIT, <timestamp>, [SEC-3008], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: FCS member moved from position <Old FCS position> to <New FCS position>.`

Probable Cause Indicates the fabric configuration server (FCS) list has been modified. One of the members of the list has been moved to a new position in the list, as identified in the message.

Recommended Action Verify the modification was planned. If the modification was planned, no action is required. If the modification was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3009

Message `AUDIT, <timestamp>, [SEC-3009], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Security Transaction aborted.`

Probable Cause Indicates the pending security transaction was aborted.

Recommended Action Verify the security transaction was intentionally aborted. If the security transaction was intentionally aborted, no action is required. If the security transaction was not intentionally aborted, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3010

Message `AUDIT, <timestamp>, [SEC-3010], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Reset [<Name of security stat(s) reset>] security stat(s).`

Probable Cause Indicates a user has reset all the security statistics.

Recommended Action Verify the security statistics were intentionally reset. If the security statistics were intentionally reset, no action is required. If the security statistics were not intentionally reset, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3011

Message `AUDIT, <timestamp>, [SEC-3011], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Reset [<Stat name>] statistics on domains [<Domain IDs>].`

Probable Cause Indicates that a user has reset a security statistic on the specified domains.

Recommended Action Verify that the security statistic was intentionally reset. If the security statistic were intentionally reset, no action is required. If the security statistic was not intentionally reset, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3012

Message

```
AUDIT, <timestamp>, [SEC-3012], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: Temp Passwd
<Password Set or Reset> on domain [<Domain ID>] for account [<Account name>].
```

Probable Cause Indicates a user has reset the password for the specified user accounts.

Recommended Action Verify the password was intentionally reset. If the password was intentionally reset, no action is required. If the password was not intentionally reset, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3013

Message

```
AUDIT, <timestamp>, [SEC-3013], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: Security Version
stamp is reset.
```

Probable Cause Indicates a user has reset the security version stamp.

Recommended Action Verify the security version stamp was intentionally reset. If the security event was planned, no action is required. If the security version stamp was not intentionally reset, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3014

Message

```
AUDIT, <timestamp>, [SEC-3014], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: <Event option>
RADIUS server <Server Name> for AAA services.
```

Probable Cause Indicates a user has changed the remote authentication dial-in user service (RADIUS) configuration.

Recommended Action Verify the RADIUS configuration was changed intentionally. If the RADIUS configuration was intentionally changed, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3015

Message `AUDIT, <timestamp>, [SEC-3015], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Moved RADIUS server <Server name> to position <New position>.`

Probable Cause Indicates a user has changed the position of the remote authentication dial-in user service (RADIUS) server.

Recommended Action Verify the RADIUS server position was intentionally changed. If the RADIUS server position was intentionally changed, no action is required. If the RADIUS server position was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3016

Message `AUDIT, <timestamp>, [SEC-3016], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Attribute [<Attribute Name>] of RADIUS server <server ID> changed <Attribute related info, if any>.`

Probable Cause Indicates a user has changed the specified attribute of the remote authentication dial-in user service (RADIUS) server.

Recommended Action Verify the RADIUS attribute was intentionally changed. If the RADIUS attribute was intentionally changed, no action is required. If the RADIUS attribute was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3017

Message `AUDIT, <timestamp>, [SEC-3017], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <Event Related Info>.`

Probable Cause Indicates a user has changed the remote authentication dial-in user service (RADIUS) configuration.

Recommended Action Verify the RADIUS configuration was intentionally changed. If the RADIUS configuration was intentionally changed, no action is required. If the RADIUS configuration was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3018

Message `AUDIT, <timestamp>, [SEC-3018], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Parameter [<Parameter Name>] changed from [<Old Value>] to [<New Value>].`

Probable Cause Indicates the specified **passwdCfg** parameter is changed.

Recommended Action Verify the **passwdCfg** parameter was intentionally changed. If the **passwdCfg** parameter was intentionally changed, no action is required. If the **passwdCfg** parameter was not intentionally changed, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3019

Message `AUDIT, <timestamp>, [SEC-3019], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Passwdcfg parameters set to default values.`

Probable Cause Indicates the **passwdCfg** parameters are set to default values.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3020

Message `AUDIT, <timestamp>, [SEC-3020], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Successful login attempt via <connection method and IP Address>.`

Probable Cause Indicates a successful login occurred. An IP address is displayed when the login occurs over a remote connection.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3021

Message `AUDIT, <timestamp>, [SEC-3021], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: failed, Info: Failed login attempt via <connection method and IP Address>.`

Probable Cause Indicates a failed login attempt occurred.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3022

Message

```
AUDIT, <timestamp>, [SEC-3022], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: Successful logout
by user [<User>].
```

Probable Cause Indicates the specified user has successfully logged out.

Recommended Action No action is required.

Severity INFO

SEC-3023

Message

```
AUDIT, <timestamp>, [SEC-3023], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: failed, Info: Account [<User>]
locked, failed password attempts exceeded.
```

Probable Cause Indicates the maximum number of failed password entries has been exceeded. The account has been locked as a result.

Recommended Action The account may automatically unlock after the lockout duration has expired or an administrator may manually unlock the account.

Severity INFO

SEC-3024

Message

```
AUDIT, <timestamp>, [SEC-3024], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: User account
[<User Name>], password changed.
```

Probable Cause Indicates the user's password was changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3025

Message `AUDIT, <timestamp>, [SEC-3025], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: User account [<User Name>] added. Role: [<Role Type>], Password [<Password Expired or not>], Home AD [<Home AD>], AD list [<AD membership List>].`

Probable Cause Indicates a new user account was created.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3026

Message `AUDIT, <timestamp>, [SEC-3026], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: User account [<User Name>], role changed from [<Old Role Type>] to [<New Role Type>].`

Probable Cause Indicates a user account role was changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3027

Message `AUDIT, <timestamp>, [SEC-3027], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: User account [<User Name>] [<Changed Attributes>].`

Probable Cause Indicates user account properties were changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3028

Message `AUDIT, <timestamp>, [SEC-3028], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: User account [<User Name>] deleted.`

Probable Cause Indicates the specified user account was deleted.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3029

Message

```
AUDIT, <timestamp>, [SEC-3029], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: Backup user
account \"<User Account Name>\" recovered.
```

Probable Cause Indicates that back user accounts were recovered.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3030

Message

```
AUDIT, <timestamp>, [SEC-3031], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info:<Event Specific
Info>
```

Probable Cause Indicates the specified **secCertUtil** operation was performed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3031

Message

```
AUDIT, <timestamp>, [SEC-3031], INFO, SECURITY, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: Distributed<List
of Databases> db(s) to <Number of domains> domains, dom-id(s)<List of Domains>.
```

Probable Cause Indicates that the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3032

Message `AUDIT, <timestamp>, [SEC-3032], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Switch is configured to <accept or reject> <Database name> database.`

Probable Cause Indicates the specified event has occurred to accept or reject a certain database.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3033

Message `AUDIT, <timestamp>, [SEC-3033], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: fddcfg --fabwideset, Status: success, Info: Fabric wide configuration set to <Fabric-wide configuration set by user>.`

Probable Cause Indicates the specified event has occurred.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3034

Message `AUDIT, <timestamp>, [SEC-3034], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: aaaconfig, Status: success, Info: Authentication configuration changed from <Previous Mode> to <Current Mode>.`

Probable Cause Indicates an authentication configuration has changed.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3035

Message `AUDIT, <timestamp>, [SEC-3035], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: ipfilter, Status: success, Info: <IP Filter Policy> IP filter policy(ies) saved.`

Probable Cause Indicates the specified IP filter policies have been saved.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3036

Message `AUDIT, <timestamp>, [SEC-3036], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: ipfilter, Status: failed, Info: Failed to save changes for <IP Filter Policy> ipfilter policies.`

Probable Cause Indicates the specified IP filter policies have not been saved.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3037

Message `AUDIT, <timestamp>, [SEC-3037], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: ipfilter, Status: success, Info: <IP Filter Policy> ipfilter policy activated.`

Probable Cause Indicates the specified IP filter policy has been activated.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3038

Message `AUDIT, <timestamp>, [SEC-3038], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: ipfilter, Status: failed, Info: Failed to activate <IP Filter Policy>.`

Probable Cause Indicates the specified IP filter policy failed to activate.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3039

Message `AUDIT, <timestamp>, [SEC-3039], INFO, SECURITY, <event-initiator-details>, <event-location>, , Event: Securty Violation, Status: failed, Info: Unauthorized host with IP address <IP address of the violating host> tries to establish connection using <Protocol Connection Type>.`

Probable Cause Indicates a security violation was reported. The IP address of the unauthorized host is displayed in the message.

Recommended Action Check for unauthorized access to the switch through the specified protocol connection. Take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3044

Message `AUDIT, <timestamp>, [SEC-3044], INFO, SECURITY, <event-initiator-details>, <event-location>, FIPS mode has been changed to <Fips Mode>.`

Probable Cause Indicates there was a change in the FIPS mode.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3045

Message `AUDIT, <timestamp>, [SEC-3045], INFO, SECURITY, <event-initiator-details>, <event-location>, System has been zeroized.`

Probable Cause Indicates the system has been zeroized.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3046

Message `AUDIT, <timestamp>, [SEC-3046], INFO, SECURITY, <event-initiator-details>, <event-location>, FIPS self tests mode has been set to <Self Test Mode>.`

Probable Cause Indicates there was a change in the FIPS Self Test mode.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3047

Message `AUDIT, <timestamp>, [SEC-3047], INFO, SECURITY, <event-initiator-details>, <event-location>, RBAC permission denied for CLI : <Cmd Name>.`

Probable Cause Indicates the user does not have permission to execute this command.

Recommended Action Verify the user has the required permission to execute this command.

Severity INFO

SEC-3048

Message `AUDIT, <timestamp>, [SEC-3048], INFO, SECURITY, <event-initiator-details>, <event-location>, FIPS mode has been enabled in the system using force option.`

Probable Cause Indicates the system has been forced to FIPS mode.

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3049

Message `AUDIT, <timestamp>, [SEC-3049], INFO, SECURITY, <event-initiator-details>, <event-location>, Status of bootprom access is changed using fipscfg CLI to : <Access Status>.`

Probable Cause Indicates the status of bootprom access is changed using the **fipscfg** command.

Recommended Action No action is required.

Severity INFO

SEC-3050

Message `AUDIT, <timestamp>, [SEC-3050], INFO, SECURITY, Event: <Event Name>, Status: success, Info: <Event Specific Info>.`

Probable Cause Indicates the specified **sshutil** operation was performed..

Recommended Action Verify the security event was planned. If the security event was planned, no action is required. If the security event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

SEC-3051

Message
```
AUDIT, <timestamp>, [SEC-3051], INFO, SECURITY, <event-initiator-details>,
<event-location>, , The license key <key> is <Action>.
```

Probable Cause Indicates that a license key is added or removed.

Recommended Action No action is required.

Severity INFO

SEC-3061

Message
```
<timestamp>, [SEC-3061], <sequence-number>, AUDIT, INFO, <system-name>, Role
<role name> is created.
```

Probable Cause Indicates a role name was created.

Recommended Action No action is required.

Severity INFO

SEC-3062

Message
```
<timestamp>, [SEC-3062], <sequence-number>, AUDIT, INFO, <system-name>, Role
<role name> is deleted.
```

Probable Cause Indicates a role name was deleted.

Recommended Action No action is required.

Severity INFO

SEC-3063

Message
```
<timestamp>, [SEC-3063], <sequence-number>, AUDIT, INFO, <system-name>, Role
<role name> is copied from <source role>.
```

Probable Cause Indicates a role name is copied from source role.

Recommended Action No action is required.

Severity INFO

SEC-3064

Message
```
<timestamp>, [SEC-3064], <sequence-number>, AUDIT, INFO, <system-name>,
Permission to the RBAC class(es) <RBAC Class Names> is changed for the role <Role
Name>.
```

Probable Cause Indicates the permission to the RBAC class is changed for the role name.

Recommended Action No action is required.

Severity INFO

SEC-3065

Message
```
<timestamp>, [SEC-3065], <sequence-number>, AUDIT, INFO, <system-name>,
Configuration of user-defined roles is uploaded.
```

Probable Cause Indicates the configuration of user-defined roles are uploaded.

Recommended Action No action is required.

Severity INFO

SEC-3066

Message
```
<timestamp>, [SEC-3066], <sequence-number>, AUDIT, INFO, <system-name>,
Configuration of user-defined roles is downloaded.
```

Probable Cause Indicates the configuration of user-defined roles are downloaded.

Recommended Action No action is required.

Severity INFO

SEC-4001

Message
```
<timestamp>, [SEC-4001], <sequence-number>, AUDIT, INFO, <system-name>, Client
logged in <IP Address> <User Account> <Application>.
```

Probable Cause Indicates the client has logged in.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT SNMP System Messages

126

SNMP-1004

Message `AUDIT, <timestamp>, [SNMP-1004], ERROR, CONFIGURATION, <event-initiator-details>, <event-location>, , Incorrect SNMP configuration.`

Probable Cause Indicates that the simple network management protocol (SNMP) configuration s incorrect and the SNMP service will not work correctly.

Recommended Action Reset the SNMP configuration to default.

Severity ERROR

SNMP-1005

Message `AUDIT, <timestamp>, [SNMP-1005], INFO, CONFIGURATION, <event-initiator-details>, <event-location>, , SNMP configuration attribute, <Changed attribute>, has changed from <Old Value> to <New Value>`

Probable Cause Indicates that the simple network management protocol (SNMP) configuration has changed as indicated. The parameter that was modified is displayed as well as the old and new values for that parameter.

Recommended Action Execute the **snmpConfig --show** command to display the new configuration.

Severity INFO

SNMP-1006

Message `AUDIT, <timestamp>, [SNMP-1006], INFO, CONFIGURATION, <event-initiator-details>, <event-location>, , <SNMP Configuration group> configuration was reset to default.`

Probable Cause Indicates that the simple network management protocol (SNMP) configuration group was reset to the factory default.

Recommended Action Execute the **snmpConfig --show** command to display the new group configuration.

Severity INFO

Chapter

AUDIT SPM System Messages

127

SPM-3001

Message `AUDIT, <timestamp>, [SPM-3001], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Node initialized.`

Probable Cause Indicates a node was initialized.

Recommended Action No action is required.

Severity INFO

SPM-3002

Message `AUDIT, <timestamp>, [SPM-3002], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: EE in slot <slot> initialized.`

Probable Cause Indicates an encryption engine was initialized.

Recommended Action No action is required.

Severity INFO

SPM-3003

Message `AUDIT, <timestamp>, [SPM-3003], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: EE in slot <slot> registered.`

Probable Cause Indicates an encryption engine was registered.

Recommended Action No action is required.

Severity INFO

SPM-3004

Message `AUDIT, <timestamp>, [SPM-3004], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: EE in slot <slot> enabled.`

Probable Cause Indicates an encryption engine was enabled.

Recommended Action No action is required.

Severity INFO

SPM-3005

Message

```
AUDIT, <timestamp>, [SPM-3005], INFO, <event-initiator-details>,
<event-location>,,Event: cryptocfg Status: success, Info: EE in slot <slot>
disabled.
```

Probable Cause Indicates an encryption engine was disabled.

Recommended Action No action is required.

Severity INFO

SPM-3006

Message

```
AUDIT, <timestamp>, [SPM-3006], INFO, <event-initiator-details>,
<event-location>,,Event: cryptocfg Status: success, Info: <source file> file
exported via scp: <hostUsername> [<hostIP>]:<hostPath>.
```

Probable Cause Indicates a file was exported via SCP protocol.

Recommended Action No action is required.

Severity INFO

SPM-3007

Message

```
AUDIT, <timestamp>, [SPM-3007], INFO, <event-initiator-details>,
<event-location>,,Event: cryptocfg Status: success, Info: <source file> file
imported via scp: <hostUsername> [<hostIP>]:<hostPath>.
```

Probable Cause Indicates a file was imported via SCP protocol.

Recommended Action No action is required.

Severity INFO

SPM-3008

Message `AUDIT, <timestamp>, [SPM-3008], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: DH challenge generated for vault IP <vaultIP>.`

Probable Cause Indicates a DH challenge was generated for a key vault.

Recommended Action No action is required.

Severity INFO

SPM-3009

Message `AUDIT, <timestamp>, [SPM-3009], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: DH response accepted.`

Probable Cause Indicates a DH challenge was accepted.

Recommended Action No action is required.

Severity INFO

SPM-3010

Message `AUDIT, <timestamp>, [SPM-3010], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: EE in slot <slot> zeroized.`

Probable Cause Indicates an encryption engine was zeroized.

Recommended Action No action is required.

Severity INFO

SPM-3011

Message `AUDIT, <timestamp>, [SPM-3011], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Local file \"<filename>\" deleted.`

Probable Cause Indicates a locally stored file was deleted.

Recommended Action No action is required.

Severity INFO

SPM-3012

Message `AUDIT, <timestamp>, [SPM-3012], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: <primaryOrSecondary> key vault registered.  Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\" IP address: <IPAddress>.`

Probable Cause Indicates a key vault was registered.

Recommended Action No action is required.

Severity INFO

SPM-3013

Message `AUDIT, <timestamp>, [SPM-3013], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Key vault with certificate label \"<certLabel>\" deregistered.`

Probable Cause Indicates a key vault was deregistered.

Recommended Action No action is required.

Severity INFO

SPM-3014

Message `AUDIT, <timestamp>, [SPM-3014], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Key archive client registered with certificate file \"<certFilename>\".`

Probable Cause Indicates a KAC certificate was registered.

Recommended Action No action is required.

Severity INFO

SPM-3015

Message `AUDIT, <timestamp>, [SPM-3015], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Key vault type set to <keyVaultType>.`

Probable Cause Indicates the key vault type was set.

Recommended Action No action is required.

Severity INFO

SPM-3016

Message `AUDIT, <timestamp>, [SPM-3016], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Master key generated.`

Probable Cause Indicates a master key was generated.

Recommended Action No action is required.

Severity INFO

SPM-3017

Message `AUDIT, <timestamp>, [SPM-3017], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Master key exported.`

Probable Cause Indicates a master key was exported.

Recommended Action No action is required.

Severity INFO

SPM-3018

Message `AUDIT, <timestamp>, [SPM-3018], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: <currentOrAlternate>master key recovered.`

Probable Cause Indicates a master key was recovered.

Recommended Action No action is required.

Severity INFO

SPM-3019

Message `AUDIT, <timestamp>, [SPM-3019], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: System card registered. Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Probable Cause Indicates a system card was registered.

Recommended Action No action is required.

Severity INFO

SPM-3020

Message `AUDIT, <timestamp>, [SPM-3020], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: System card with certificate label \"<certLabel>\" deregistered.`

Probable Cause Indicates a system card was deregistered.

Recommended Action No action is required.

Severity INFO

SPM-3021

Message `AUDIT, <timestamp>, [SPM-3021], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Authentication card registered.  Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Probable Cause Indicates an authentication card was registered.

Recommended Action No action is required.

Severity INFO

SPM-3022

Message `AUDIT, <timestamp>, [SPM-3022], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Authentication card with certificate label \"<certLabel>\" deregistered.`

Probable Cause Indicates an authentication card was deregistered.

Recommended Action No action is required.

Severity INFO

SPM-3023

Message `AUDIT, <timestamp>, [SPM-3023], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: System card <enabledOrDisabled>.`

Probable Cause Indicates use of the system card was enabled or disabled.

Recommended Action No action is required.

Severity INFO

SPM-3024

Message `AUDIT, <timestamp>, [SPM-3024], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Quorum size set to <quorumsize>.`

Probable Cause Indicates the quorum size was set.

Recommended Action No action is required.

Severity INFO

SPM-3025

Message `AUDIT, <timestamp>, [SPM-3025], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: File imported via usb: Source: <sourcePath> Destination: <destinationFilename>.`

Probable Cause Indicates a file was imported via USB device.

Recommended Action No action is required.

Severity INFO

SPM-3026

Message `AUDIT, <timestamp>, [SPM-3026], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: File exported via usb: Source: <sourcePath> Destination: <destinationFilename>.`

Probable Cause Indicates a file was exported via USB device.

Recommended Action No action is required.

Severity INFO

SPM-3027

Message `AUDIT, <timestamp>, [SPM-3027], INFO, <event-initiator-details>, <event-location>,,Event: cryptocfg Status: success, Info: Recovery card registered.  Certificate label: \"<certLabel>\" Certificate file: \"<certFilename>\".`

Probable Cause Indicates a recovery card was registered.

Recommended Action No action is required.

Severity INFO

SPM-3028

Message `AUDIT, <timestamp>, [SPM-3028], <sequence-number>,, INFO, <system-name>, Event: SPM-EE state changed, Info: EE State: <EE Status>.`

Probable Cause Indicates an EE state has changed.

Recommended Action No action is required.

Severity INFO

SPM-3029

Message `AUDIT, <timestamp>, [SPM-3029], <sequence-number>,, INFO, <system-name>, Event: KeyVault Connection Status: <status>, Info:KAC_Connect: <kac status>.`

Probable Cause Indicates the status of key vault.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT SULB System Messages

128

SULB-1001

Message `AUDIT, <timestamp>, [SULB-1001], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwaredownload command has started.`

Probable Cause Indicates the **firmwareDownload** command has been started. This process should take approximately 17 minutes. The process is set to time out after 30 minutes.

Recommended Action No action is required. Allow the **firmwareDownload** command to continue without disruption. Do not fail over or power down the system during firmware upgrade.

Run the **firmwareDownloadStatus** command for more information.

Severity WARNING

SULB-1002

Message `AUDIT, <timestamp>, [SULB-1002], INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwaredownload command has completed successfully.`

Probable Cause Indicates the **firmwareDownload** command has completed successfully and switch firmware has been updated.

Recommended Action No action is required. The **firmwareDownload** command has completed as expected.

Run the **firmwareDownloadStatus** command for more information. Run the **firmwareShow** command to verify the firmware versions.

Severity INFO

SULB-1003

Message `AUDIT, <timestamp>, [SULB-1003], INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwarecommit has started.`

Probable Cause Indicates that the **firmwareCommit** command has started.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1004

Message `AUDIT, <timestamp>, [SULB-1004], INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwarecommit has completed.`

Probable Cause Indicates the **FirmwareCommit** command is executed.

Recommended Action No action is required. Run the **firmwareDownloadStatus** command for more information.

Severity INFO

SULB-1009

Message `AUDIT, <timestamp>, [SULB-1009], INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwaredownload command failed. status: 0x<status code>, error: 0x<error code>.`

Probable Cause Indicates the **firmwareDownload** command failed. The additional *status code* and *error code* provide debugging information.

Table lists **firmwareDownload** status messages and status codes. Some of them will not show up in this RASLOG message. They are listed for the sake of completeness.

TABLE 9 Status Messages and Status Codes

Status Message	Status Code
"**firmwareDownload** sanity check failed."	0x30
"Sanity check failed because system is non-redundant."	0x31
"Sanity check failed because **firmwareDownload** is already in progress."	0x32
"Sanity check failed because FABRIC OS is disabled on Active CP."	0x33
"Sanity check failed because HAMD is disabled on Active CP."	0x34
"Sanity check failed because **firmwareDownload** is already in progress."	0x35
"Sanity check failed because FABRIC OS is disabled on Standby CP."	0x36
"Sanity check failed because HAMD is disabled on Standby CP."	0x37
"**firmwareDownload** failed on Standby CP."	0x40
"**firmwareDownload** failed on Standby CP."	0x41
"**firmwareDownload** failed on Standby CP."	0x42
"**firmwareCommit** failed on Standby CP."	0x43
"**firmwareDownload** failed."	0x44
"**firmwareDownload** failed due to IPC error."	0x50
"Unable to check the firmware version on Standby CP due to IPC error."	0x51
"**firmwareDownload** failed due to IPC error."	0x52
"**firmwareDownload** failed due to IPC error."	0x53
"Standby CP failed to reboot due to IPC error."	0x54

TABLE 9 Status Messages and Status Codes

Status Message	Status Code
“**firmwareCommit** operation failed due to IPC error.”	0x55
"Unable to check the firmware version on Standby CP due to IPC error."	0x56
“Unable to restore the original firmware due to Standby CP timeout.”	0x57
"Standby CP failed to reboot and was not responding."	0x58
"Unable to check the firmware version on Standby CP due to IPC error."	0x59
“Sanity check failed because **firmwareDownload** is already in progress.”	0x60
“Sanity check failed because **firmwareDownload** is already in progress.”	0x61
NOT USED	0x62
"System Error."	0x63
"Active CP forced failover succeeded. Now this CP becomes Active."	0x64
"Standby CP booted up."	0x65
"Active and Standby CP failed to gain HA synchronization within 10 minutes."	0x66
"Standby rebooted successfully."	0x67
"Standby failed to reboot."	0x68
“**firmwareCommit** has started to restore the secondary partition.”	0x69
"Local CP is restoring its secondary partition."	0x6a
“Unable to restore the secondary partition. Please use **firmwareDownloadStatus** and **firmwareShow** to see firmware status.”	0x6b
“**firmwareDownload** has started on Standby CP. It might take up to 10 minutes.”	0x6c
“**firmwareDownload** has completed successfully on Standby CP.”	0x6d
"Standby CP reboots."	0x6e
"Standby CP failed to boot up."	0x6f
"Standby CP booted up with new firmware."	0x70
"Standby CP failed to boot up with new firmware."	0x71
“**firmwareDownload** has completed successfully on Standby CP.”	0x72
“**firmwareDownload** has started on Standby CP. It might take up to 10 minutes.”	0x73
“**firmwareDownload** has completed successfully on Standby CP.”	0x74
"Standby CP reboots."	0x75
"Standby CP failed to reboot."	0x76
“**firmwareCommit** has started on Standby CP.”	0x77
“**firmwareCommit** has completed successfully on Standby CP.”	0x78
"Standby CP booted up with new firmware."	0x79
"Standby CP failed to boot up with new firmware."	0x7a
“**firmwareCommit** has started on both Active and Standby CPs.”	0x7b
“**firmwareCommit** has completed successfully on both CPs.”	0x7c
“**firmwareCommit** failed on Active CP.”	0x7d

TABLE 9 Status Messages and Status Codes

Status Message	Status Code
"The original firmware has been restored successfully on Standby CP."	0x7e
"Unable to restore the original firmware on Standby CP."	0x7f
"Standby CP reboots."	0x80
"Standby CP failed to reboot."	0x81
"Standby CP booted up with new firmware."	0x82
"Standby CP failed to boot up with new firmware."	0x83
"There was an unexpected reboot during **firmwareDownload**. The command is aborted."	0x84
"Standby CP was not responding. The command is aborted."	0x85
"**firmwareCommit** has started on both CPs. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status."	0x86
"**firmwareCommit** has started on the local CP. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status."	0x87
"**firmwareCommit** has started on the remote CP. Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status."	0x88
"Please use **firmwareDownloadStatus** and **firmwareShow** to see the firmware status."	0x89
"**firmwareDownload** command has completed successfully."	0x8a
"The original firmware has been restored successfully."	0x8b
"Remote CP is restoring its secondary partition."	0x8c
"Local CP is restoring its secondary partition."	0x8d
"Remote CP is restoring its secondary partition."	0x8e
"**firmwareDownload** has started."	0x8f
"**firmwareCommit** has started."	0x90
"**firmwareDownload** has completed successfully."	0x91
"**firmwareCommit** has completed successfully."	0x92
"**firmwareCommit** has started to restore the secondary partition."	0x93
"**firmwareCommit** failed."	0x94
"The secondary partition has been restored successfully."	0x95
"Firmware is being downloaded to the blade. This step may take up to 10 minutes."	0xa0
"**firmwareDownload** timed out."	0xa1
"Reboot occurred during **firmwareDownload**. **firmwareCommit** will be started to recover the blade."	0xa2
"Blade rebooted during **firmwareCommit**. The operation will be restarted."	0xa3
"Firmware has been downloaded successfully. Blade is rebooting with the new firmware."	0xa4
"Blade has rebooted successfully."	0xa5
"New firmware failed to boot up. Please retry **firmwareDownload**."	0xa6
"**firmwareCommit** has started on the blade. This may take up to 10 minutes."	0xa7

TABLE 9 Status Messages and Status Codes

Status Message	Status Code
“**firmwareRestore** is entered. System will reboot and a **firmwareCommit** operation will start upon boot up.”	0xa8
"Switch is relocating the AP image."	0xa9
"The AP image is relocated successfully."	0xaa
"Switch reboots during relocating the AP image. The operation will be restarted."	0xab
“Blade failed to reboot with the original image. **firmwareRestore** command failed.”	0xac

Table lists additional **firmwareDownload** error messages and error codes. They provide more details on why **firmwareDownload** failed.

TABLE 10 Error Messages and Error Codes

Error Message	Error Code
"Image is up-to-date. No need to download the same version of firmware."	0xF
“Upgrade is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding.”	0x10
“OSRootPartition is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding. For example: swap OSRootPartitions and reboot.”	0x11
“Unable to access the required package list file. Check whether the switch is supported by the requested firmware. Also check **firmwareDownload** help page for other possible failure reasons.”	0x12
"The RPM package database is inconsistent. Contact your service provider for recovery."	0x13
"Out of memory."	0x14
"Failed to download RPM package."	0x15
"Unable to create firmware version file."	0x16
"Unexpected system error."	0x17
“Error in getting lock device for **firmwareDownload**.”	0x18
“Error in releasing lock device for **firmwareDownload**.”	0x19
“**firmwareCommit** failed.”	0x1a
"Firmware directory structure is not compatible. Check whether the firmware is supported on this platform."	0x1b
"Failed to load the Linux kernel image."	0x1c
“OSLoader is inconsistent. Run the **bootEnv** (root) command to correct the inconsistency before proceeding.”	0x1d
“New image has not been committed. Run **firmwareCommit** or **firmwareRestore** first and then try **firmwareDownload**.”	0x1e
“**firmwareRestore** failed.”	0x1f
"Both images are mounted to the same device."	0x20
“Unable to unionist old packages.”	0x21
“**firmwareDownload** is already in progress.”	0x22

TABLE 10 Error Messages and Error Codes

Error Message	Error Code
“**firmwareDownload** timed out.”	0x23
"Our of disk space."	0x24
“Primary filesystem is inconsistent. Run **firmwareRestore** to restore the original firmware, or contact your service provider for recovery.”	0x25
"The post-install script failed."	0x26
"Unexpected reboot."	0x27
"Primary kernel partition is inconsistent. Please contact your service provider for recovery."	0x28
"The pre-install script failed."	0x29
“The platform option is not supported. Run **chassisConfig** to reset the option first and then try **firmwareDownload**.”	0x2a
"Failed to install RPM package."	0x2b
"Cannot downgrade directly to this version. Downgrade to an intermediate version first and then download the desired version."	0x2c
“Cannot download 5.1 because Device Based Routing policy is not supported by 5.1. Use **aptPolicy** to change the routing policy before proceeding.”	0x2d
"Invalid RPM package. Please reload firmware packages on the file server."	0x2e
"Cannot downgrade due to presence of blade type 17. Remove or power off these blades before proceeding."	0x2f
"Cannot downgrade due to presence of blade type 24. Remove or power off these blades before "	0x30
"Cannot downgrade due to presence of long-distance ports in LS mode. Please remove these settings before proceeding."	0x31
"Network is not reachable. Please verify the IP address of the server is correct."	0x32

The following section explains the causes of some common error messages:

0x15 - Failed to download Red Hat package manager (RPM) package. If this error occurs immediately after **firmwareDownload** is started, the firmware on the switch may be two releases older than the requested firmware. **firmwareDownload** supports firmware upgrades within two feature releases (a feature release is indicated by a major number and a minor number, for example, X.Y). The following are major upgrade versions for the Fabric OS: v4.0, v4.1, v4.2, v4.4, v5.0, v5.1.,5.2, and 5.3. In this case, you will need to upgrade to an intermediate version before downloading the desired version. If this error occurs in the middle of **firmwareDownload**, the firmware in the file server may be corrupted or there may be a temporary network issue. In this case, retry the **firmwareDownload** command. If the problem persists, contact your system administrator.

0x18 - Error in getting lock device for **firmwareDownload**. This error may occur because another **firmwareDownload** is already in progress. Run **firmwareDownloadStatus** to verify that this is the case. Wait for the current session to finish before proceeding.

0x23 - **firmwareDownload** timed out. This error may occur because **firmwareDownload** has not completed within the predefined timeout period. It is most often caused by network issues. If the problem persists, contact your system administrator.

0x24 - out of disk space. This error may occur because some coredump files have not been removed from the filesystem and are using up disk space. Remove these coredump files using the **supportSave** command before proceeding.

0x29 - The pre-install script failed. This error may be caused by an unsupported blade type in the chassis. Remove or power off the unsupported blades before proceeding. Another possible cause may be an invalid **chassisConfig** option setting. In that case, reset the **chassisConfig** option before retrying **firmwareDownload**.

0x2e - Invalid Red Hat package manager (RPM) package. This error maybe caused by an inconsistent firmware image loaded on the file server. It may also be caused by temporary networking issues. Please reload firmware packages on the file server, then retry **firmwareDownload**. If the problem persists, contact your system administrator.

Table 11 lists the **firmwareDownload** state names and state values. They indicate where in the **firmwareDownload** process the error occurred.

TABLE 11 Upgrade State and Code Value

Upgrade State	Code
SUS_PEER_CHECK_SANITY	0x21
SUS_PEER_FWDL_BEGIN	0x22
SUS_SBY_FWDL_BEGIN	0x23
SUS_PEER_REBOOT	0x24
SUS_SBY_REBOOT	0x25
SUS_SBY_FABOS_OK	0x26
SUS_PEER_FS_CHECK	0x27
SUS_SELF_FAILOVER	0x28
SUS_SBY_FWDL1_BEGIN	0x29
SUS_SELF_FWDL_BEGIN	0x2a
SUS_SELF_COMMIT	0x2b
SUS_SBY_FWC_BEGIN	0x2c
SUS_SBY_COMMIT	0x2d
SUS_SBY_FS_CHECK	0x2e
SUS_ACT_FWC_BEGIN	0x2f
SUS_PEER_RESTORE_BEGIN	0x30
SUS_SBY_RESTORE_BEGIN	0x31
SUS_PEER_FWC_BEGIN	0x32
SUS_PEER_FS_CHECK1	0x33
SUS_FINISH	0x34
SUS_COMMIT	0x35

Recommended Action

Run the **firmwareDownloadStatus** command for more information.

In a director-class switch, when **firmwareDownload** fails, the command will synchronize the firmware on the two partitions of each CP by starting a firmware commit operation. Wait until this operation completes (about 10 minutes) before attempting another **firmwareDownload**.

In a director-class switch, when **firmwareDownload** fails, the two CPs may end up with different versions of firmware and they may not gain high-availability (HA) sync. In that case, run **firmwareDownload** single mode (-s) to upgrade the firmware on the standby CP to the same version as the active CP. Then retry **firmwareDownload** to download the desired version of firmware onto the CPs.

Refer to the *Fabric OS Administrator's Guide* for troubleshooting information.

Severity INFO

SULB-1010

Message `AUDIT, <timestamp>, [SULB-1010], INFO, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwarecommit failed (status=0x<error code>).`

Probable Cause Indicates the **firmwareCommit** command has failed. The error code provides debugging information. See Table 11 for more information.

Recommended Action If the failure is caused by an inconsistent filesystem, contact your switch service provider.

Severity INFO

SULB-1017

Message `AUDIT, <timestamp>, [SULB-1017], ERROR, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwaredownload failed in slot <Slot number>.`

Probable Cause Indicates the **firmwareDownload** command has failed in the specified blade. The error may be caused by an inconsistent AP blade firmware stored on the active CP. It may also be caused by an internal Ethernet issue or by a persistent storage hardware failure.

Recommended Action Run the **slotShow** command. If the blade is in FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload** to the blade. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1018

Message `AUDIT, <timestamp>, [SULB-1018], ERROR, FIRMWARE, <event-initiator-details>, <event-location>, , Firmwaredownload timed out in slot <Slot number>.`

Probable Cause Indicates there may be an error caused by a blade initialization issue after the new firmware is downloaded and the blade is rebooted. The error may also be caused by an internal Ethernet issue or by a persistent storage failure.

Recommended Action Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload**. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1020

Message `AUDIT, <timestamp>, [SULB-1020], ERROR, FIRMWARE, <event-initiator-details>, <event-location>, , New firmware failed to boot in slot <Slot number>.`

Probable Cause Indicates the BP blade should restart with the new image, but is still running the old image. This error may indicate that the new image has not been loaded correctly to the specified blade.

Recommended Action Run the **slotShow** command. If the blade is in a FAULTY state, run the **slotPowerOff** and **slotPowerOn** commands to trigger another **firmwareDownload** to the blade. If the blade is stuck in LOADING state, remove and re-insert the blade to trigger another **firmwareDownload**. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1021

Message `AUDIT, <timestamp>, [SULB-1021], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Firmware is being downloaded to the blade in slot <Slot number>.`

Probable Cause Indicates the firmware is being loaded to the specified blade.

Recommended Action Run the **firmwareDownloadStatus** command to monitor the **firmwareDownload** progress. After it finishes, run the **firmwareShow** command to verify the firmware versions.

Severity WARNING

SULB-1023

Message `AUDIT, <timestamp>, [SULB-1023], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , The blade in slot <Slot number> has rebooted during firmwaredownload.`

Probable Cause Indicates there may be an error caused by an unexpected disruption of the **firmwareDownload** command, for example, by powering off and on of the indicated BP blade in the middle of a **firmwareDownload**. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended Action The **firmwareCommit** command will be started automatically after the blade boots up to repair the secondary partition. If at the end of **firmwareCommit**, the blade firmware version is still inconsistent with the active CP firmware, **firmwareDownload** will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress. If the problem persists, contact your switch service provider.

Severity WARNING

SULB-1024

Message `AUDIT, <timestamp>, [SULB-1024], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Firmware commit has completed on the blade in slot <Slot number>.`

Probable Cause Indicates the **firmwareCommit** operation has completed on the specified blade.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. If the blade firmware is the same as the active CP firmware, **firmwareDownload** has completed successfully on the blade. However, if the **firmwareCommit** operation has been started to repair the secondary partition, at the end of **firmwareCommit**, the blade firmware version may still be inconsistent with the active CP firmware. In that case, **firmwareDownload** will automatically be restarted on the blade. Run the **firmwareDownloadStatus** command to monitor the progress.

Severity WARNING

SULB-1026

Message `AUDIT, <timestamp>, [SULB-1026], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Firmware commit operation started on the blade in slot <Slot number>.`

Probable Cause Indicates the **firmwareCommit** command has started on the specified blade. The operation may be a normal part of **firmwareDownload**, or it may have started to repair the secondary partition of the blade if the secondary partition is corrupted.

Recommended Action Wait for the commit operation to complete.

Severity WARNING

SULB-1030

Message `AUDIT, <timestamp>, [SULB-1030], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , The switch has rebooted during relocating the internal firmware image.`

Probable Cause Indicates there may be an error caused by an unexpected disruption of the **firmwareDownload** command, for example, by powering the switch off and on in the middle of a **firmwareDownload**. The error may also be caused by persistent storage hardware failure or by a software error.

Recommended Action The **firmwareDownload** command will continue after the switch has rebooted. Run the **firmwareDownloadStatus** command to monitor progress. If the problem persists, contact your switch service provider.

Severity WARNING

SULB-1031

Message `AUDIT, <timestamp>, [SULB-1032], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Relocating an internal firmware image on the CP.`

Probable Cause Indicates the switch has rebooted with the new firmware and is relocating the AP firmware.

Recommended Action Wait for the operation to complete.

Severity WARNING

SULB-1032

Message `AUDIT, <timestamp>, [SULB-1032], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Relocating an internal firmware image on the CP.`

Probable Cause Indicates the switch has started firmware download to the co-CPU.

Recommended Action Wait for the operation to complete.

Severity WARNING

SULB-1033

Message `AUDIT, <timestamp>, [SULB-1033], WARNING, FIRMWARE, <event-initiator-details>, <event-location>, , Switch has completed relocating the internal firmware image.`

Probable Cause Indicates the **firmwareDownload** process has completed on the switch.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. Run the **switchShow** command to make sure the switch is enabled.

Severity WARNING

SULB-1034

Message `AUDIT, <timestamp>, [SULB-1034], ERROR, FIRMWARE, <event-initiator-details>, <event-location>, Relocation of internal image timed out.`

Probable Cause Indicates there may be an error caused by a switch initialization issue after the internal image is relocated. It may also be caused by an internal Ethernet issue or by persistent storage failure.

Recommended Action Reboot the switch. This will cause the internal image to be relocated again. Use the **firmwareDownloadStatus** command to monitor the progress. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1035

Message `AUDIT, <timestamp>, [SULB-1035], ERROR, FIRMWARE, <event-initiator-details>, <event-location>, , An error has occurred during relocation of the internal image.`

Probable Cause Indicates an error has occurred during the relocation of the internal image. The error may be caused by inconsistent internal firmware image. It may also be caused by the internal Ethernet or persistent storage hardware failure.

Recommended Action Reset the switch. This will cause the internal image to be relocated again. If the problem persists, contact your switch service provider.

Severity ERROR

SULB-1037

Message `AUDIT, <timestamp>, [SULB-1037], ERROR, FIRMWARE, HCL failed. Reboot the switch manually using the reboot command. However, it will disrupt the FC traffic.`

Probable Cause Indicates HCL has failed. Many reasons, such as domain not confirmed, can cause this failure.

Recommended Action Run the **reboot** command to restart the switch manually.

Severity ERROR

SULB-1038

Message `AUDIT, <timestamp>, [SULB-1038], WARNING, FIRMWARE, Co-CPU has not booted up properly. Skip the firmwaredownload command on the co-CPU.`

Probable Cause Indicates that the Main CPU cannot access the co-CPU to update the firmware on the co-CPU or run any other firmwaredownload command on the co-CPU. If firmwareDownload in progress it will continue without updating the co-CPU firmware.

Recommended Action After firmwaredownload completes, reboot the CP manually to bring up the co-CPU and run the **firmwareDownload** command again. If the problem persists, contact the service provider.

Severity WARNING

SULB-1039

Message `AUDIT, <timestamp>, [SULB-1039], INFO, FIRMWARE, CP has completed relocating the internal firmware image.`

Probable Cause Indicates that the firmwareDownload command process has been completed normally on the CP.

Recommended Action Run the **firmwareShow** command to verify the firmware versions.

Severity INFO

SULB-1040

Message `AUDIT, <timestamp>, [SULB-1040], INFO, WARNING, An error has occurred during relocation of the internal image on the CP.`

Probable Cause Indicates an error has occurred during the relocation of the internal image. The error may be caused by inconsistent internal firmware image. It may also be caused by the internal Ethernet failure.

Recommended Action Run the **firmwareShow** command to verify the firmware versions. Run the **firmwareDownload** command again if the firmware is not updated.

This will cause the internal image to be relocated again. If the problem persists, contact your switch service provider.

Severity WARNING

Chapter

AUDIT SWCH System Messages

129

SWCH-1012

Message `AUDIT, <timestamp>, [SWCH-1012], INFO, CFG, <event-initiator-details>, <event-location>, , Trunk Area (<trunk area>) has been enabled for one or more ports.`

Probable Cause Indicates a Trunk Area has been enabled for one or more ports and the config file has been updated.

Recommended Action No action is required.

Severity INFO

SWCH-1013

Message `AUDIT, <timestamp>, [SWCH-1013], INFO, CFG, <event-initiator-details>, <event-location>, , Trunk Area has been disabled for one or more ports.`

Probable Cause Indicates Trunk Area assignment has been disabled for one or more ports and the config file has been updated.

Recommended Action No action is required.

Severity INFO

SWCH-1014

Message `AUDIT, <timestamp>, [SWCH-1014], INFO, CFG, <event-initiator-details>, <event-location>, , All Trunk Areas have been disabled.`

Probable Cause Indicates all Trunk Areas have been disabled and the config file has been updated.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT UCST System Messages

130

UCST-1021

Message `AUDIT, <timestamp>, [UCST-1021], INFO, CFG, <event-initiator-details>, <event-location>, , In-order delivery option has been enabled.`

Probable Cause Indicates the IOD option has been enabled for the switch. This option guarantees in-order delivery of frames during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1022

Message `AUDIT, <timestamp>, [UCST-1022], INFO, CFG, <event-initiator-details>, <event-location>, , In-order delivery option has been disabled.`

Probable Cause Indicates the IOD option has been disabled for the switch. This may cause out-of-order delivery of frames.

Recommended Action No action is required.

Severity INFO

UCST-1023

Message `AUDIT, <timestamp>, [UCST-1023], INFO, CFG, <event-initiator-details>, <event-location>, , Dynamic Load Sharing option has been enabled.`

Probable Cause Indicates the DLS option has been enabled for the switch. This will move existing routes to a new redundant path, when this path becomes available.

Recommended Action No action is required.

Severity INFO

UCST-1024

Message `AUDIT, <timestamp>, [UCST-1024], INFO, CFG, <event-initiator-details>, <event-location>, , Dynamic Load Sharing option has been disabled.`

Probable Cause Indicates the DLS option has been disabled for the switch.

Recommended Action No action is required.

Severity INFO

UCST-1025

Message `AUDIT, <timestamp>, [UCST-1025], INFO, CFG, <event-initiator-details>, <event-location>, , In-order delivery option has been enabled with Lossless-DLS option.`

Probable Cause Indicates the IOD option has been enabled for the switch. This option guarantees in-order delivery of frames during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1026

Message `AUDIT, <timestamp>, [UCST-1026], INFO, CFG, <event-initiator-details>, <event-location>, ,LossLess-DLS option has been enabled.`

Probable Cause Indicates that the *NoFrameDrop* option is enabled. This will help minimizing frame loss during topology changes.

Recommended Action No action is required.

Severity INFO

UCST-1027

Message `AUDIT, <timestamp>, [UCST-1027], INFO, CFG, <event-initiator-details>, <event-location>, , LossLess-DLS option has been disabled.`

Probable Cause Indicates that the *NoFrameDrop* option is disabled. This may cause higher frame loss during topology changes.

Recommended Action No action is required.

Severity INFO

Chapter

AUDIT ZONE System Messages 131

ZONE-3001

Message

```
AUDIT, <timestamp>, [ZONE-3001], INFO, ZONE, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: <Zone object type>
\"<Zone object member list>\" added to <Zone object set type> \"<Zone object set
name>\".
```

Probable Cause Indicates that a new zone object member or members have been added to the specified zone object set.

The *zone object type* can be "alias", "zone member", "zone" or "zone configuration". The string "..." appears at the end of the zone object member list if the list was truncated in the message.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3002

Message

```
AUDIT, <timestamp>, [ZONE-3002], INFO, ZONE, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: <Zone object set
type> \"<Zone object set name>\" created with <Zone object type> \"<Zone object
member list>\".
```

Probable Cause Indicates a new zone object set was created and the specified zone object member or members were added to that new zone object set.

The *zone object type* can be "alias", "zone member", "zone" or "zone configuration". The string "..." appears at the end of the zone object member list if the list was truncated in the message.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3003

Message

```
AUDIT, <timestamp>, [ZONE-3003], INFO, ZONE, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: <Zone object type>
\"<Zone object name>\" deleted.
```

Probable Cause Indicates the specified zone object has been deleted.

The *zone object type* can be “alias”, “zone member”, “zone” or “zone configuration”. The string “...” appears at the end of the zone object member list if the list was truncated in the message.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3004

Message

```
AUDIT, <timestamp>, [ZONE-3004], INFO, ZONE, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: <Zone object type>
\"<Zone object member list>\" removed from <Zone object set type> \"<Zone object
set name>\".
```

Probable Cause Indicates the specified zone object member or members have been removed from the specified zone object set.

The *zone object type* can be “alias”, “zone member”, “zone” or “zone configuration”. The string “...” appears at the end of the zone object member list if the list was truncated in the message.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3005

Message

```
AUDIT, <timestamp>, [ZONE-3005], INFO, ZONE, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: All zone
information cleared from transaction buffer.
```

Probable Cause Indicates all zone information has been cleared from the transaction buffer.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3006

Message

```
AUDIT, <timestamp>, [ZONE-3006], INFO, ZONE, <event-initiator-details>,
<event-location>, , Event: <Event Name>, Status: success, Info: Current zone
configuration disabled. <AD Id>.
```

Probable Cause Indicates the current zone configuration has been disabled.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3007

Message `AUDIT, <timestamp>, [ZONE-3007], INFO, ZONE, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Zone configuration \"<Zone configuration>\" enabled. <AD Id>.`

Probable Cause Indicates the specified zone configuration has been enabled.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3008

Message `AUDIT, <timestamp>, [ZONE-3008], INFO, ZONE, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Current zone configuration saved to MRAM. <AD Id>.`

Probable Cause Indicates the current zone configuration has been successfully saved to magnetoresistive random access memory (MRAM).

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3009

Message `AUDIT, <timestamp>, [ZONE-3009], INFO, ZONE, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <Event Description>.`

Probable Cause Indicates the specified zone transaction has been aborted.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3010

Message `AUDIT, <timestamp>, [ZONE-3010], INFO, ZONE, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" copied to new zone object \"<New Zone object name>\".`

Probable Cause Indicates the specified zone object has been copied to a new zone object.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3011

Message `AUDIT, <timestamp>, [ZONE-3011], INFO, ZONE, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" expunged.`

Probable Cause Indicates the specified zone object has been expunged.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3012

Message `AUDIT, <timestamp>, [ZONE-3012], INFO, ZONE, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Zone object \"<Zone object name>\" renamed to \"<New Zone object name>\".`

Probable Cause Indicates the specified zone object has been renamed.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3013

Message `AUDIT, <timestamp>, [ZONE-3013], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <Admin domain name> has been activated.`

Probable Cause Indicates the specified admin domain (AD) has been activated.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3014

Message `AUDIT, <timestamp>, [ZONE-3014], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: \"<AD object member list>\" added to <AD object set type> \"<AD object set name>\".`

Probable Cause Indicates the specified new admin domain (AD) object member or members have been added to the specified AD object set.

An *AD object set type* is “AD member”. The string “...” appears at the end of the AD object member list if the list was truncated in the message.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3015

Message `AUDIT, <timestamp>, [ZONE-3015], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: AD configurations applied.`

Probable Cause Indicates the current admin domain (AD) configuration has been saved to flash is being enforced.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3016

Message `AUDIT, <timestamp>, [ZONE-3016], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: All AD definitions cleared.`

Probable Cause Indicates all admin domain (AD) definitions and all zone configurations under them have been cleared.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3017

Message `AUDIT, <timestamp>, [ZONE-3017], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <AD object set type> \"<AD object set name>\" created with \"<AD object member list>\".`

Probable Cause Indicates the specified admin domain (AD) has been created.

An *AD object set type* is “AD member”. The string “...” appears at the end of the AD object member list if the list was truncated in the message.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3018

Message `AUDIT, <timestamp>, [ZONE-3018], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <AD object name> has been deactivated.`

Probable Cause Indicates the specified admin domain (AD) object has been deactivated.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3019

Message `AUDIT, <timestamp>, [ZONE-3019], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: <AD object type> \"<AD object name>\" deleted.`

Probable Cause Indicates the specified admin domain (AD) object has been deleted.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3020

Message `AUDIT, <timestamp>, [ZONE-3020], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: \"<AD object member list>\" removed from <AD object set type> \"<AD object set name>\".`

Probable Cause Indicates the specified admin domain (AD) member or members have been removed from an AD.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3021

Message `AUDIT, <timestamp>, [ZONE-3021], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: AD object \"<AD object name>\" renamed to \"<New AD object name>\".`

Probable Cause Indicates the specified admin domain (AD) has been renamed.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3022

Message `AUDIT, <timestamp>, [ZONE-3022], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: success, Info: Current AD configuration saved to flash.`

Probable Cause Indicates the current admin domain (AD) configuration has been saved to flash.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3023

Message `AUDIT, <timestamp>, [ZONE-3023], INFO, FABRIC, <event-initiator-details>, <event-location>, , Event: <Event Name>, Status: Failure, Info: AD Apply operation failed due to transaction conflict.`

Probable Cause Indicates the admin domain **ad --apply** operation failed due to a transaction conflict.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3024

Message `AUDIT, <timestamp>, [ZONE-3024], INFO, FABRIC, <event-initiator-details>, <event-location>, , Command: <Command Name>, Status: success, Info: executed. <AD Id>.`

Probable Cause Indicates the admin domain **ad --transabort** operation was successful in the specified AD.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

Severity INFO

ZONE-3025

Message `AUDIT, <timestamp>, [ZONE-3025], INFO, FABRIC, <event-initiator-details>, <event-location>, , Command: <Command Name> Info: executed. In AD <AD Id>.`

Probable Cause Indicates the admin domain **ad --exec** operation was executed in the specified AD.

Recommended Action Verify the event was planned. If the event was planned, no action is required. If the event was not planned, take appropriate action as defined by your enterprise security policy.

131 ZONE-3025

Severity INFO