Release Notes for TopspinOS Release 2.6.0 FCS

Release Date: July 28, 2006
Part Number: OL-9388-04

Contents

This document contains these sections:

Introduction

These release notes describe the features and known issues for the TopspinOS 2.6.0 FCS (build 195 for 4x switch module and build 198 for 1x switch module) and Element Manager 2.6.0.6 software releases.

Note These release notes apply to the Cisco 4x InfiniBand Switch Module for IBM BladeCenter and Cisco InfiniBand Switch Module for IBM BladeCenter switches that run TopspinOS 2.6.0 software.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

System Requirements

This section describes the system requirements for this software release.

Determining the Software Version

To determine the version of the operating system that you are running on the switch, log in to the CLI and enter the **show version** EXEC command.

```
SFS-7000P> show version
================================================================================
                            System Version Information
================================================================================
system-version : Cisco-BCH TopspinOS 2.6.0 releng #195 …
contact : support@ibm.com
name : Cisco BladeCenterH
```

Upgrading to a New Software Release

To verify that you are running the latest available release, compare your version against the latest version on the Cisco support website at http://www.cisco.com/cgi-bin/tablebuild.pl/sfs-bladecenter. After registering your product, you should have received a username and password that grant you access to this site.

Switch software and Linux host drivers are now released and packaged separately. Switch software is also now packaged and released separately for the following products:

- Cisco SFS 7000, 7000P, 7008, and 7008P chassis—2.7.0 FCS
- Topspin 120 and 270 chassis—2.7.0 FCS
- 4X InfiniBand Switch Module for IBM BladeCenter H—2.6.0 FCS
- 1X InfiniBand Switch Module for IBM BladeCenter—2.6.0 FCS
- Cisco SFS 3001 and 3012 I/O chassis—2.4.0 Update 1
- Topspin 90 and 360 I/O chassis—2.4.0 Update 1

The TopspinOS 2.6.0 release supports 3.0.0 (or higher) Linux host drivers. The 3.0.0 Linux host drivers require that all switches first be upgraded to TopspinOS 2.1.0 or higher.

Old and new TopspinOS releases can be used in the same InfiniBand fabric, although InfiniBand subnet manager synchronization will not occur between TopspinOS 2.2.0 and newer releases.

Switches should be upgraded before the InfiniBand hosts.

To upgrade Element Manager (EM) GUI, first uninstall previous software release and then install software release 2.6.0.

For general information about upgrading to a new software release, see the Install Software Images section in the *Cisco SFS 7000 Series Product Family Chassis Manager User Guide* and the *Cisco 4x InfiniBand Switch Module for IBM BladeCenter User Guide.*

New and Changed Information

TopspinOS 2.6.0 is a major release that introduces significant new features and documentation. It includes the following changes:

- Support for TACACS+ authentication
- Secure copy (scp) file transfers
- Multiple RADIUS servers and secondary syslog server
- Many bug fixes

Changes Since Software Release 2.5.0 Update 1 (build 251)

This section describes the new features and resolved caveats since the 2.5.0 Update 1 (build 251) release.

Note The ID number from the Cisco Defect Tracking System, if applicable, is included with this format: CSCxxyyyyy. The current status of all issues is available online at http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. Contact Cisco Technical Support for more information.

InfiniBand

- CSCsd57775

  Added support for viewing the InfiniBand Linear Forwarding Table (LFT) and Multicast Forwarding Table (MFT) to SNMP, Element Manager GUI, and CLI.

- CSCsd55622

  Added support for configuring several more InfiniBand Subnet Manager parameters.

Management

- CSCtp06345

  Fixed a problem in upgrading TopspinOS where BladeCenter Management Module would see a fault with diagnostic code 0x15.

- CSCsd43751

  Added support for viewing Cisco-standard Unique Device Indentifier Information with the new **show inventory** CLI command.

- CSCsd57699

  Added support for authentication with TACACS+.

- CSCsd54558

  Added support for secondary syslog server.

- CSCsd73467

  Added support for up to three RADIUS servers.

- CSCsd89599

  Added support for displaying a CLI login banner through the optional **config:login-banner** file.

- CSCtp05680

  The **show card-inventory** CLI command now displays uptime (number of seconds since booting) for each card.

- CSCtp02078, CSCsd68686, CSCsd68674, CSCse00615, CSCse08205, CSCse08216

  Several problems were fixed in hardware fault error reporting.

Changes Since Software Release 2.5.0 FCS (build 241)

This section describes the new features and resolved caveats since the 2.5.0 FCS (build 241) release.

Note The ID number from the Cisco Defect Tracking System, if applicable, is included with this format: CSCxxyyyyy. The current status of all issues is available online at http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl. Contact Cisco Technical Support for more information.

InfiniBand

- CSCsd10909

  Fixed a problem in which the sm-info information about other InfiniBand subnet managers could be incorrect after a fabric merge.

- CSCsd34069

  Fixed a problem in route calculation for heterogeneous InfiniBand fabrics that use a mixture of 1X, 4X, and 12X links.

Management

- CSCsd29798, CSCsd29835, CSCsd31190, CSCsd31289

  Fixed several problems in Chassis Manager Web GUI.

- CSCsd33064

  Fixed a problem in Element Manager GUI in which multiple diagnostic tests could not be run.

Changes Since Software Release 2.3.0 FCS (build 222)

This section describes the new features and resolved caveats since the 2.3.0 FCS (build 222) release.

InfiniBand

- CSCtp04427, CSCtp06472

  InfiniBand packet lifetimes are now configurable.

- CSCtp06383

  An InfiniBand subnet manager crash under heavy load has been fixed.

- CSCsc46269

  The performance of the InfiniBand subnet manager has been improved.

- CSCsc49085

  The InfiniBand subnet manager now has improved route calculation for heterogeneous InfiniBand fabrics that use a mixture of 1X, 4X, and 12X links.

- CSCtp06908

  Support for viewing the other InfiniBand subnet managers in a subnet has been added to SNMP, Element Manager GUI, and the new **show ib sm sm-info** CLI command.

- CSCtp06909

  Support for viewing the InfiniBand event subscribers in a subnet has been added to SNMP, Element Manager GUI, and the new **show ib sm subscription** CLI command.

- CSCsc46206

  Support has been added for configuring the maximum number of hops (depth) that the InfiniBand subnet manager has to search when configuring the InfiniBand fabric. This feature can be used to increase Subnet Manager performance on large fabrics.

Management

- CSCsd05202

  A problem has been fixed that caused the management Ethernet port to stop working.

- CSCtp06503

  Support for secure copy (scp) has been added.

- CSCsc46894

  Support for Cisco Discovery Protocol (CDP) has been added.

- CSCtp06811

  Added additional SNMP traps for Power On Self-Test (POST) failures.

- CSCtp04448

  Added additional SNMP traps for power supply up and fan up events.

Changes Since Software Release 2.2.0 Update 1 (build 545)

This section describes the new features and resolved caveats since the 2.2.0 update 1 (build545) release.

InfiniBand

- CSCtp06338

  Support for user-configurable InfiniBand multicast groups has been added.

- CSCtp06557

  A Performance Management (PM) memory leak has been fixed. This memory leak, which occurred over time when monitoring was enabled or port counters were retrieved many times, could exhaust system memory and cause a chassis reboot.

- CSCtp05747

  The management InfiniBand interface now supports a nondefault InfiniBand subnet prefix.

- CSCtp06358

  A problem has been fixed where a synchronized standby Subnet Manager shutting down could cause the master Subnet Manager to stall.

- CSCtp06312

  Several scenarios have been fixed where a master and standby Subnet Manager could get out of synchronization.

Management

- CSCtp05653

  The diagnostic card **self test** command has been fixed to not run out of system resources if it is repeatedly started and stopped before the command has completed.

- The **show diag post** and **show diag fru-error** commands now report descriptive values for problems instead of integer error codes.

Caveats

This section describes temporary limitations of this release. These restrictions will be resolved in a future release of this product.

InfiniBand

- CSCtp05858

  In autonegotiation mode, it is possible for an unconnected InfiniBand port to report errors if the port is part of a cluster of three ports, where at least one of the other ports is connected.

Management

- CSCtp06068

  The addr-option value for the InfiniBand switch module Ethernet management interface should alwaydynamic. Setting addr-option to static or dhcp will cause the BladeCenter Management Module to lose communication with the Switch Module.

- CSCse39550

  CLI ssh logins do not authenticate with RADIUS or TACACS+.

- CSCtp04462, CSCtp05567, CSCtp05620

  The **diagnostic interface ib** commands are not supported.

- CSCtp05816

  It is possible for POST to detect a fan that is not completely plugged in, but the error does not show up in the **show diag post** or **show diag fru-error** command output. The error is reported in the hwif_log.

- CSCtp01801

  If a firmware upgrade fails, the CLI does not report why the failure occurred.

  Workaround: Use the **show logging end** command to review the failure.

- CSCtp02078

  The error messages in the **show logging** command for environmental monitoring failures, such as failed power supplies, are cryptic.

- CSCtp00813

  The CLI does not provide any diagnostics if the NTP server(s) is not responding.

- CSCtp01498

  After executing the CLI **delete** or **clock set** commands, the CLI **reload** command will unnecessarily prompt if you wish to save changes.

- CSCtp02196

  The EM GUI will not install if there is not sufficient temporary space in /tmp.

- CSCtp01285

  The Serial/Mgmt-Ethernet and Maintenance->System Info windows in the GUI may not display if the GUI has been running for a while.

- CSCtp01977

  The ALT-TAB icon for the Element Manager GUI is blank on Linux.

Related Documentation

The following list describes the documentation available with TopspinOS 2.6.0, which is available in electronic form and printed form upon request.

Note Documentation is included on the TopspinOS 2.6.0 Server Switch CD Image.

You can download the latest documentation updates on the Cisco support site at http://www.cisco.com/en/US/partner/products/ps6418/tsd_products_support_category_home.html.

- *InfiniBand Hardware Installation and Cabling Guide*
- *Cisco 4x InfiniBand Switch Module for IBM BladeCenter User Guide*
- *Release Notes for TopspinOS Release 2.6.0*
- *Cisco SFS 7000 Series Product Family Chassis Manager User Guide*
- *Cisco SFS 7000 Series Product Family Element Manager User Guide*
- *Cisco SFS 7000 Series Product Family Command Reference Guide*

Service and Support

For additional support, you must first register your product at http://www.cisco.com. After registering, you may contact your supplier for support, or Cisco directly.

Refer to the "Obtaining Technical Assistance" section on page 11 in this document.

When you call Cisco Technical Support or use the Cisco Technical Support website at http://www.cisco.com, be prepared to provide the following information to support personnel:

General Information

- Technical Support registration number, if applicable
- Error messages received
- Detailed description of the problem and specific questions
- Description of any troubleshooting steps already performed and results

Server Configuration

- Type of server, chip set, CPU, amount of RAM, and number of nodes
- Attached storage devices (output from cat /proc/scsi/scsi)
- InfiniBand configuration (output from /usr/local/topspin/sbin/hca_self_test)

Chassis Configuration

- Chassis model
- Output from the **show running-status all** command

Chassis Serial Number

The chassis serial number and corresponding bar code are provided on the serial number label, as shown in this example:

Model: TS360

SN UST323XXXXXXXXX

This chassis serial number can be found on the bottom of the chassis or the outside of the chassis box packaging. It can also be found in the output of the **show backplane** command.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.