



Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.2(2c)

Release Date: February 5, 2008

Part Number: OL-14116-03 Q0

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the “[Related Documentation](#)” section on [page 49](#).



Note

Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*:
http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_release_notes_list.html

[Table 1](#) shows the on-line change history for this document.

Table 1 **Online History Change**

Revision	Date	Description
A0	10/06/2007	Created release notes.
B0	02/05/2008	Added DDTS CSCsm54598 .
C0	04/22/2008	Added DDTS CSCsl72080 .
D0	04/30/2008	Added DDTS CSCso63465 .
E0	06/26/2008	Added DDTS CSCsl04532 . Added Caution: Upgrading from Cisco MDS SAN-OS Release 3.0(3) with SSI Release 3.0(3i) to SAN-OS Release 3.2(2c) with SSI Release 3.2(3k) will be disruptive .
F0	07/09/2008	Added Upgrading to Recover Loss of Performance Manager Data . Added NPIV Requirements .
G0	09/16/2008	Added DDTS CSCsl53091 .
H0	09/17/2008	Added DDTS CSCsl12611 .



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

© 2008 Cisco Systems, Inc. All rights reserved.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 1 Online History Change

Revision	Date	Description
I0	11/13/2008	Added the “Performing a Nondisruptive Software Upgrade on Generation 1 Modules” section.
J0	11/18/2008	Added DDTS CSCso72230 . Removed DDTS CSCsk90998 .
K0	01/15/2009	Added the “Changes in Existing Features” section, which includes information about iSNS server and iSNS client features being deprecated.
L0	04/14/2009	Updated DDTS CSCsk49634 .
M0	04/29/2009	Added “FICON Supported Releases and Upgrade Paths”. Revised “FICON Downgrade Paths”. Added the “Compatibility of Fabric Manager and Data Mobility Manager” limitation.
N0	08/28/2009	Added a Note to the “Upgrading Your Version of Cisco Fabric Manager” section on page -13 about the effect of a Group Policy Object (GPO) in Windows on Fabric Manager Server when used with the PostgreSQL database.
O0	07/29/2010	Added the “PPRC Not Supported with FCIP Write Acceleration” limitation. Added the “Using IVR In a Fabric With Mixed Code Versions” limitation.
P0	11/03/2010	Added the Supervisor-2A module to Table 2 .
Q0	02/04/2011	Changed the status of DDTS CSCsk00953 to Resolved.

Contents

This document includes the following sections:

- [Introduction, page 3](#)
- [Components Supported, page 3](#)
- [Software Download Process, page 9](#)
- [Upgrading Your Cisco MDS SAN-OS Software Image, page 12](#)
- [Downgrading Your Cisco MDS SAN-OS Software Image, page 23](#)
- [New Features in Cisco MDS SAN-OS Release 3.2\(2c\), page 26](#)
- [Changes in Existing Features, page 28](#)
- [Limitations and Restrictions, page 29](#)
- [Caveats, page 35](#)
- [Related Documentation, page 49](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 51](#)

Send documentation comments to mdsfeedback-doc@cisco.com

Introduction

The Cisco MDS 9000 Family of Multilayer Directors and Fabric Switches provides industry-leading availability, scalability, security, and management, allowing you to deploy high performance storage-area networks with lowest total cost of ownership. Layering a rich set of intelligent features onto a high performance, protocol agnostic switch fabric, the Cisco MDS 9000 Family addresses the stringent requirements of large data center storage environments: uncompromising high availability, security, scalability, ease of management, and seamless integration of new technologies.

The Cisco MDS 9000 Family SAN-OS is the underlying system software that powers the Cisco MDS 9500 Series, 9200 Series, and 9100 Series multilayer switches. The Cisco SAN-OS provides intelligent networking features, such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

Components Supported

Table 2 lists the SAN-OS software part number and hardware components supported by the Cisco MDS 9000 Family.



Note

To use the Cisco Storage Services Enabler package, Cisco MDS SAN-OS Release 1.3(5) or later must be installed on the MDS switch.

Table 2 *Cisco MDS 9000 Family Supported Software and Hardware Components*

Component	Part Number	Description	Applicable Product
Software	M95S2K9-3.2.2	MDS 9500 Supervisor/Fabric-2, SAN-OS software.	MDS 9500 Series only
	M95S1K9-3.2.2	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S2K9-3.2.2	MDS 9222 Supervisor/Fabric-2, SAN-OS software.	MDS 9200 Series only
	M92S1K9-3.2.2	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S2K9-3.2.2	MDS 9100 Supervisor/Fabric-2, SAN-OS software.	MDS 9100 Series only
	M91S1K9-3.2.2	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
License	M9500ENT1K9	Enterprise package.	MDS 9500 Series
	M9200ENT1K9	Enterprise package.	MDS 9200 Series
	M9100ENT1K9	Enterprise package.	MDS 9100 Series
	M9500FIC1K9	Mainframe package.	MDS 9500 Series
	M9200FIC1K9	Mainframe package.	MDS 9200 Series
	M9100FIC1K9	Mainframe package.	MDS 9100 Series
	M9100FIC1EK9	FICON license.	MDS 9100 Series
	M9500FMS1K9	Fabric Manager Server package.	MDS 9500 Series
	M9200FMS1K9	Fabric Manager Server package.	MDS 9200 Series
	M9100FMS1K9	Fabric Manager Server package.	MDS 9100 Series
	M9500EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9500 Series
	M9200EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9200 Series
	M9500EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9500 Series
	M9200EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9200 Series
	M9500EXT12K9	SAN Extension over IP package for MPS-14/2 module.	MDS 9500 Series
	M9200EXT12K9	SAN Extension over IP package for MPS-14/2 module.	MDS 9200 Series
	M9500EXT1AK9	SAN Extension over IP package for MSM-18/4 module or MSFM-18/4 FIPS module.	MDS 9500 Series
	M9200EXT1AK9	SAN Extension over IP package for MSM-18/4 module or MSFM-18/4 FIPS module.	MDS 9200 Series
	M9500SSE1K9	Storage Services Enabler package.	MDS 9500 Series with SSM
	M9200SSE1K9	Storage Services Enabler package.	MDS 9200 Series with SSM
	M9500SME1MK9	Cisco Storage Media Encryption package for MSM-18/4 module	MDS 9500 Series with MSM
	M9200SME1MK9	Cisco Storage Media Encryption package for MSM-18/4 module	MDS 9200 Series with MSM
	M9200SME1FK9	Cisco Storage Media Encryption package for fixed slot	MDS 9222i Switch only
	M95DMMS1K9	Data Mobility Manager (DMM)	MDS 9500 Series with SSM

Send documentation comments to mdsfeedback-doc@cisco.com

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
License	M92DMMS1K9	Data Mobility Manager (DMM)	MDS 9200 Series with SSM
	M95DMMTS1K9	Data Mobility Manager (DMM) for 180 days	MDS 9500 Series with SSM
	M92DMMTS1K9	Data Mobility Manager (DMM) for 180 days	MDS 9200 Series with SSM
	M9124PL8-4G	On-Demand Ports Activation License	MDS 9124 Switch
	M9134PL8-4G	On-Demand Ports Activation License	MDS 9134 Switch
	M9134PL2-10G	On-Demand Ports Activation License	MDS 9134 Switch
	HP-PL12-4G	On-Demand Ports Activation License	Cisco Fabric Switch for HP c-Class BladeSystem only
	IBM-PL10-4G	On-Demand Ports Activation License	Cisco Fabric Switch for IBM BladeCenter only
Chassis	DS-C9513	MDS 9513 director (13-slot modular chassis with 11 slots for switching modules, and 2 slots reserved for Supervisor 2 modules only—SFPs ¹ sold separately).	MDS 9513 Switch only
	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9509 Switch only
	DS-C9506	MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9506 Switch only
	DS-C9222i-K9	MDS 9222i Multiservice Modular Switch (includes 18 4-Gbps Fibre Channel ports and 4 Gigabit Ethernet IP storage services ports, and a modular expansion slot for Cisco MDS 9000 Family Switching and Service modules.)	MDS 9222i Switch only
	DS-C9216-K9	MDS 9216 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216 Switch only
	DS-C9216A-K9	MDS 9216A 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216A Switch only
	DS-C9216i-K9	MDS 9216i 16-port semi-modular fabric switch (includes 14 1-Gbps/2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216i Switch only
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports).	MDS 9140 Switch only

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Chassis	DS-C9124-K9	MDS 9124 fixed configuration (non-modular) multilayer fabric switch (includes 8 enabled ports; an on-demand ports activation license can enable 8 additional ports, up to 24 ports).	MDS 9124 Switch only
	DS-C9134-K9	MDS 9134 fixed configuration (non-modular) multilayer fabric switch (includes 24 enabled 4-Gbps ports; an on-demand ports activation license can enable 8 additional ports, up to 32 4-Gbps ports. An additional port activation license can enable 2 10-Gbps ports.).	MDS 9134 Switch only
	DS-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 Switch only
	DS-HP-FC-K9	Cisco Fabric Switch for HP c-Class BladeSystem (includes sixteen internal and eight external active ports and four 4-Gb SFPs installed, or eight internal and four external active ports and two 4-Gb SFPs installed).	Cisco Fabric Switch for HP c-Class BladeSystem only
	DS-IBM-FC-K9	Cisco Fabric Switch for IBM BladeCenter (includes fourteen internal and six external ports)	Cisco Fabric Switch for IBM BladeCenter only
External crossbar module	DS-13SLT-FAB1	MDS 9513 crossbar fabric module.	MDS 9513 Switch only
Supervisor modules	DS-X9530-SF2-K9	MDS 9500 Supervisor-2, module.	MDS 9500 Series only
	DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A module.	
	DS-X9530-SF1-K9	MDS 9500 Supervisor/Fabric-I module.	
Switching modules	DS-X9016	MDS 9000 16-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series
	DS-X9032	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	
	DS-X9112	MDS 9000 12-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X9124	MDS 9000 24-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X9148	MDS 9000 48-port 4-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X9704	MDS 9000 4-port 10-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch

Send documentation comments to mdsfeedback-doc@cisco.com

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP Storage services module.	MDS 9500 Series and 9200 Series
	DS-X9304-SMIP	4-port Gigabit Ethernet IP Storage services module.	
	DS-X9032-SSM	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	
	DS-X9304-18K9	18-port Fibre Channel/4-port Gigabit Ethernet Multiservice (MSM-18/4) module.	
	DS-X9304-18FK9	18-port Fibre Channel/4-port Gigabit Ethernet Multiservice FIPS (MSFM-18/4) module.	
Optics	DS-X2-FC10G-SR	X2/SC optics, 10-Gbps Fibre Channel for Short Reach.	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X2-FC10G-LR	X2/SC optics, 10-Gbps Fibre Channel for Long Reach.	
	DS-X2-FC10G-ER	X2/SC optics, 10-Gbps Fibre Channel for Extended Reach (40 km).	
	DS-X2-E10G-SR	X2/SC optics, 10-Gbps Ethernet for Short Reach	
	DS-X2-FC10G_CX4	X2/CX-4 optics, 10-Gbps Fibre Channel, copper	
LC-type fiber-optic SFP	DS-SFP-FC-2G-SW	2-Gbps/1-Gbps Fibre Channel—short wavelength SFP.	MDS 9000 Family
	DS-SFP-FC-2G-LW	2-Gbps/1-Gbps Fibre Channel—long wavelength SFP.	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—short wavelength SFP.	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—long wavelength SFP.	
	DS-SFP-GE-T	1-Gbps Ethernet SFP.	
	DS-SFP-FC4G-SW	4-Gbps/2-Gbps/1-Gbps Fibre Channel—short wavelength SFP for DS-X91xx switching modules.	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-SFP-FC4G-MR	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 4 km.	
	DS-SFP-FC4G-LW	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 10 km.	
CWDM ²	DS-CWDM-xxxx	Gigabit Ethernet and 1-Gbps/2-Gbps/4-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm.	MDS 9000 Family
	DS-CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths.	
	DS-CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths.	
	DS-CWDMCHASSIS	Two slot chassis for CWDM add/drop multiplexers.	

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Table 2 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
Power supplies	DS-CAC-6000W	6000-W AC power supply.	MDS 9513 only
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC power supply.	
	DS-CAC-3000W	3000-W AC power supply.	
	DS-CAC-4000W-US	4000-W AC power supply for US (cable attached).	
	DS-CAC-4000W-INT	4000-W AC power supply international (cable attached).	
	DS-CAC-1900W	1900-W AC power supply.	MDS 9506 only
	DS-CDC-1900W	1900-W DC power supply.	
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-300W	300-W ³ AC power supply.	MDS 9100 Series only
CompactFlash	MEM-MDS-FLD51M	MDS 9500 supervisor CompactFlash disk, 512 MB.	MDS 9500 Series only
Port analyzer adapter	DS-PAA-2, DS-PAA	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	MDS 9000 Family
CD-ROM	M90FMK9-CD322=	MDS 9000 Management Software and Documentation CD-ROM, spare.	MDS 9000 Family

1. SFP = small form-factor pluggable
2. CWDM = coarse wavelength division multiplexing
3. W = Watt

Send documentation comments to mdsfeedback-doc@cisco.com

Software Download Process

Use the software download procedure to upgrade to a later version, or downgrade to an earlier version, of an operating system. This section describes the software download process for the Cisco MDS SAN-OS and includes the following topics:

- [Determining the Software Version, page 9](#)
- [Downloading Software, page 9](#)
- [Selecting the Correct Software Image for an MDS 9200 Series Switch, page 10](#)
- [Migrating from Supervisor-1 Modules to Supervisor-2 Modules, page 11](#)
- [Configuring Generation 2 Switching Modules, page 11](#)

Determining the Software Version

To determine the version of Cisco MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the CLI, log in to the switch and enter the **show version EXEC** command.

To determine the version of Cisco MDS SAN-OS software currently running on a Cisco MDS 9000 Family switch using the Fabric Manager, view the Switches tab in the Information pane, locate the switch using the IP address, logical name, or WWN, and check its version in the Release column.



Note

We strongly recommend that you use the latest available software release supported by your vendor for all Cisco MDS 9000 Family products.

Downloading Software

The Cisco MDS SAN-OS software is designed for mission-critical high availability environments. To realize the benefits of nondisruptive upgrades on the Cisco MDS 9500 Directors, we highly recommend that you install dual supervisor modules.

To download the latest Cisco MDS SAN-OS software, access the Software Center at this URL:

<http://www.cisco.com/public/sw-center>

See the following sections in this release note for details on how you can nondisruptively upgrade your Cisco MDS 9000 switch. Issuing the **install all** command from the CLI, or using Fabric Manager to perform the downgrade, enables the compatibility check. The check indicates if the upgrade can happen nondisruptively or disruptively depending on the current configuration of your switch and the reason.

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
-----	-----	-----	-----	-----
1	yes	non-disruptive	rolling	
2	yes	disruptive	rolling	Hitless upgrade is not supported
3	yes	disruptive	rolling	Hitless upgrade is not supported
4	yes	non-disruptive	rolling	
5	yes	non-disruptive	reset	
6	yes	non-disruptive	reset	

At a minimum, you need to disable the default device alias distribution feature using the **no device-alias distribute** command in global configuration mode. The **show incompatibility system bootflash:1.3(x)_filename** command determines which additional features need to be disabled.

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

Refer to the “Determining Software Compatibility” section of the [Cisco MDS 9000 Family CLI Configuration Guide](#) for more details.

**Note**

If you would like to request a copy of the source code under the terms of either GPL or LGPL, please send an e-mail to mds-software-disclosure@cisco.com.

Selecting the Correct Software Image for an MDS 9100 Series Switch

The system and kickstart image that you use for an MDS 9100 series switch depends on which switch you use, as shown in [Table 3](#).

Table 3 *Software Images for MDS 9100 Series Switch*

Switch	Image
MDS 9120 or MDS 9140	Filename begins with m9100-s1ek9
MDS 9134, MDS 9124, Cisco Fabric Switch for HP BladeSystem, or Cisco Fabric Switch for IBM BladeCenter	Filename begins with m9100-s2ek9

Selecting the Correct Software Image for an MDS 9200 Series Switch

The system and kickstart image that you use for an MDS 9200 series switch depends on which switch you use, as shown in [Table 4](#).

Table 4 *Software Images for MDS 9200 Series Switches*

Switch	Image
MDS 9222i	Filename begins with m9200-s2ek9
MDS 9216A or MDS 9216i	Filename begins with m9200-ek9

Selecting the Correct Software Image for an MDS 9500 Series Switch

The system and kickstart image that you use for an MDS 9500 Series switch depends on whether the switch is based on a Supervisor-1 module or a Supervisor-2 module, as shown in [Table 5](#).

Table 5 *Software Images for Supervisor Type*

Supervisor Type	Switch	Image
Supervisor-1 module	MDS 9506 and 9509	Filename begins with m9500-sf1ek9
Supervisor-2 module	MDS 9506, 9509, and 9513	Filename begins with m9500-sf2ek9

Use the **show module** command to display the type of supervisor module in the switch. For a Supervisor-1 module, the output might look like this:

Send documentation comments to mdsfeedback-doc@cisco.com

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  ---
...
...
5    0      Supervisor/Fabric-1        DS-X9530-SF1-K9      active*
6    0      Supervisor/Fabric-1        DS-X9530-SF1-K9      ha-standby
```

For a Supervisor-2 module, the output might look like this:

```
switch# show module
Mod  Ports  Module-Type                Model                Status
---  ---
...
...
7    0      Supervisor/Fabric-2        DS-X9530-SF2-K9      active *
8    0      Supervisor/Fabric-2        DS-X9530-SF2-K9      ha-standby
```

Migrating from Supervisor-1 Modules to Supervisor-2 Modules

As of Cisco MDS SAN-OS Release 3.0(1), the Cisco MDS 9509 and 9506 Directors support both Supervisor-1 and Supervisor-2 modules. Supervisor-1 and Supervisor-2 modules cannot be installed in the same switch, except during migration. Both the active and standby supervisor modules must be of the same type, either Supervisor-1 or Supervisor-2 modules. For Cisco MDS 9513 Directors, both supervisor modules must be Supervisor-2 modules.



Caution

Migrating your supervisor modules is a disruptive operation.



Note

Migrating from Supervisor-2 modules to Supervisor-1 modules is not supported.

To migrate from a Supervisor-1 module to a Supervisor-2 module, refer to the step-by-step instructions in the [Cisco MDS 9000 Family CLI Configuration Guide](#).

Configuring Generation 2 Switching Modules

The Cisco MDS 9500 Multilayer Directors are designed to operate with any combination of Cisco MDS 9000 Generation 1 and Generation 2 modules. However, there are limitations to consider when combining the various modules and supervisors in the Cisco MDS 9500 Series platform chassis. The references listed in this section provide specific information about configurations that combine different modules and supervisors.

For information on configuring Generation 2 switching modules, refer to:

http://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080664c6b.html

For information on port index availability, refer to:

http://www.cisco.com/en/US/products/ps5990/products_installation_guide_chapter09186a0080419599.html

For information on Cisco MDS 9000 hardware and software compatibility, refer to:

http://www.cisco.com/en/US/products/ps5989/products_device_support_table09186a00805037ee.html

Send documentation comments to mdsfeedback-doc@cisco.com

Upgrading Your Cisco MDS SAN-OS Software Image

This section lists the guidelines recommended for upgrading your Cisco MDS SAN-OS software image and contains the following sections:

- [Performing a Nondisruptive Software Upgrade on Generation 1 Modules, page 12](#)
- [Upgrading Your Version of Cisco Fabric Manager, page 13](#)
- [General Upgrading Guidelines, page 15](#)
- [Upgrading with IVR Enabled, page 18](#)
- [Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2\(2c\), page 20](#)
- [Upgrading the SSI Image on Your SSM, page 21](#)
- [Upgrading a Switch with Insufficient Space for Two Images on the Bootflash, page 21](#)
- [Upgrading a Cisco MDS 9124 Switch, page 22](#)
- [Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch, page 23](#)

Performing a Nondisruptive Software Upgrade on Generation 1 Modules

Generation 1 modules may reload during a nondisruptive SAN-OS software upgrade because of the CompactFlash being unable to partition for the new code. If that happens, the installer aborts and reloads the module.

This issue affects the following modules:

- DS-X9016, 16-port 1-Gbps/2-Gbps Fibre Channel module
- DS-X9032, 32-port 1-Gbps/2-Gbps Fibre Channel module
- DS-X9032-SSM, 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM)
- DS-X9302-14K9, 14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module

This issue might be seen during an upgrade from Cisco SAN-OS Release 3.0(x), 3.1(x) or 3.2(x). It has been addressed for upgrades from SAN-OS Release 3.3(1) or higher. Therefore, you will not be impacted by this issue if you are running SAN-OS Release 3.3(1) when you upgrade to a higher SAN-OS release.

When this problem occurs, the module will automatically reload and may cause the Install All to stop, which will cause the upgrade to be unsuccessful. Error messages similar to the following may be displayed:

```
Install has failed. Return code 0x40930020 (Non-disruptive upgrade of a module failed).
Please identify the cause of the failure, and try 'install all' again.
Module 2: Non-disruptive upgrading.
-- FAIL. Return code 0x40690009 (Error in downloading image for image upgrade).
```

To avoid this kind of unplanned disruption, follow the methods for identifying and correcting this issue described in [Cisco Field Notice 63099](#), before proceeding with the SAN-OS upgrade. This Field notice can be found under the [Support, Products page for Cisco MDS9500 Series Multilayer Directors](#) selection.

The caveat associated with this issue is CSCsm62295.

Send documentation comments to mdsfeedback-doc@cisco.com

Upgrading Your Version of Cisco Fabric Manager

As of Cisco SAN-OS Release 3.2(1), Cisco Fabric Manager is no longer packaged with a Cisco MDS 9000 Family switch. It is included on the CD-ROM that ships with the switch. You can install Fabric Manager from the CD-ROM or from files that you download.

Installing Cisco Fabric Manager is a multi-step process that involves installing a database, as well as Fabric Manager. The complete installation instructions are provided in the “Installation of Cisco MDS SAN-OS and Fabric Manager” section in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*, and are available on-screen once you launch the Fabric Manager installer from the CD-ROM.

The following section presents the flow of the installation process at a high level. Review these guidelines before you begin the installation process.

1. Verify supported software. Cisco Fabric Manager has been tested with the following software:

- Windows 2000 SP4, 2003 SP2, XP SP2
- Redhat Linux (2.6 Kernel)
- Solaris (SPARC) 8 and 10
- VMWare Server 1.0:
 - Base Operating System: Windows 2000 SP4 / Virtual Operating System: Windows XP SP2
 - Base Operating System: Windows 2000 SP4 / Virtual Operating System: Windows 2000 SP4
- Java Sun JRE and JDK 1.5(x) are supported
- Java Web Start 1.2, 1.0.1, and 1.5
- Firefox 1.5 and 2.0
- Internet Explorer 6.x, and 7.0



Note Internet Explorer 7.0 is not supported on Windows 2000 SP4.

- Oracle Database 10g Express
- PostgreSQL 8.2 (Windows and Linux)
- PostgreSQL 8.1 (Solaris)
- Cisco ACS 3.1 and 4.0
- PIX Firewall
- IP Tables
- SSH v2
- Global Enforce SNMP Privacy Encryption
- HTTPS

2. Ensure data migration when upgrading Cisco Fabric Manager from Cisco SAN-OS Releases 3.1(2b) and later.

If you are upgrading Cisco Fabric Manager in Cisco SAN-OS Releases 3.1(2b) and later, be aware that data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or Oracle Database 10g Express during the installation. Data is also migrated from Oracle Database 10g Express to Oracle Database 10g Express. If you migrate the database from Oracle to Oracle, the schema is updated.

Send documentation comments to mdsfeedback-doc@cisco.com

3. Ensure data migration when upgrading Cisco Fabric Manager from releases prior to Cisco SAN-OS Releases 3.1(2b).

If you are upgrading Fabric Manager in a Cisco SAN-OS Release prior to 3.1(2b), be aware that data is migrated from the Hypersonic HSQL database to either the PostgreSQL database or the Oracle Database 10g Express during the installation. The Fabric Manager Installer installs the PostgreSQL database on Windows. If you want to install the PostgreSQL database on Solaris or Linux, or if you want to install the Oracle Database 10g Express database, follow the instructions in the “Installation of Cisco MDS SAN-OS and Fabric Manager” section in the *Cisco MDS 9000 Family Fabric Manager Configuration Guide*.



Note

If you are upgrading a previous installation of Fabric Manager, make sure the previous installation is installed and running. Do not uninstall the previous version. If the previous version is uninstalled, the database will not be migrated and your server settings will not be preserved.

4. Select the database.

If you want to use the Oracle Database 10g Express, you must install the database and create a user name and password before continuing with the Fabric Manager installation. We recommend the Oracle Database 10g Express option for all users who are running Performance Manager on large fabrics (1000 or more end devices).

If you want to install the PostgreSQL database, you must disable any security software you are running as PostgreSQL may not install certain folders or users. You must also log in as a Superuser before you start the installation.

5. Install Fabric Manager from the CD-ROM or from files that you download from Cisco.com at the following website:

<http://cisco.com/cgi-bin/tablebuild.pl/mds-fm>

To install Fabric Manager on Solaris, follow these steps:

-
- Step 1** Set Java 1.5 to the path that is to be used for installing Fabric Manager.
 - Step 2** Install the database that is to be used with Fabric Manager.
 - Step 3** Copy the Fabric Manager jar file **m9000-fm-3.2.2c.jar** from the CD-ROM to a folder on the Solaris workstation.
 - Step 4** Launch the installer using the following command:

```
java -Xms512m -Xmx512m -jar m9000-fm-3.2.2c.jar
```
 - Step 5** Follow the onscreen instructions provided in the Fabric Manager management software setup wizard.
-

To install Fabric Manager on Windows, follow these steps:

-
- Step 1** Click the **Install Management Software** link.
 - Step 2** Choose **Management Software > Cisco Fabric Manager**.
 - Step 3** Click the **Installing Fabric Manager** link.
 - Step 4** Select the drive for your CD-ROM.
 - Step 5** Click the **FM Installer** link.

Send documentation comments to mdsfeedback-doc@cisco.com

Step 6 Follow the onscreen instructions provided in the Fabric Manager Installer 3.2(2c).



Note

If you are running Fabric Manager Server on Windows and using the PostgreSQL database, you should examine your Windows Active Directory environment for organizational units (OUs) and make the change recommended below to ensure that Fabric Manager Server does not periodically stop working.

On a Windows system, the Microsoft Active Directory applies a Group Policy Object (GPO) to the Fabric Manager Server. The GPO does not recognize the local user PostgreSQL because it is not in the GPO allow list. As a result, the GPO removes it, and the PostgreSQL database stops working.

To avoid this situation, you should move the Fabric Manager Server to its own OU and apply the same feature settings as the original OU, but remove the local user account to log in as a service.

To install Device Manager on your workstation, follow these steps:

- Step 1** Enter the IP address of the switch in the Address field of your browser.
- Step 2** Click the **Cisco Device Manager** link in the Device Manager installation window.
- Step 3** Click **Next** to begin the installation.
- Step 4** Follow the onscreen instructions to complete the installation of Device Manager.



Note

If you use a Java JDK instead of a JRE on Solaris, you might encounter a problem trying to install the Device Manager from a web browser. This can happen because the installer heap limit of 256 MB is not sufficient. If you have this problem, save the `jnlp` link as file, increase the heap limit to 512 MB, and run `javaws element-manager.jnlp` at the shell prompt.

General Upgrading Guidelines

Use the following guidelines when upgrading to Cisco MDS SAN-OS Release 3.2(2c):

- Install and configure dual supervisor modules.
- Issue the **show install all impact upgrade-image** CLI command to determine if your upgrade will be nondisruptive.
- Follow the recommended guidelines for upgrading a Cisco MDS 9124 Switch as described in [“Upgrading a Cisco MDS 9124 Switch” section on page 22](#).
- Follow the guidelines for upgrading a single supervisor switch as described in [“Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch” section on page 23](#).
- Be aware that some features impact whether an upgrade is disruptive or nondisruptive:
 - **Fibre Channel Ports:** Traffic on Fibre Channel ports can be nondisruptively upgraded. See [Table 6](#) for the nondisruptive upgrade path for all SAN-OS releases.
 - **SSM:** Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during an upgrade. SSM Fibre Channel traffic is not.

Send documentation comments to mdsfeedback-doc@cisco.com

- **Gigabit Ethernet Ports:** Traffic on Gigabit Ethernet ports is disrupted during an upgrade or downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module, the MSM-18/4 module, and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the upgrade is in progress.
- **Inter-VSAN Routing (IVR):** With IVR enabled, you must follow additional steps if you are upgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a). See the [“Upgrading with IVR Enabled” section on page 18](#) for these instructions.
- **FICON:** If you have FICON enabled, the upgrade path is different. See [Table 8](#).

Use [Table 6](#) to determine your nondisruptive upgrade path to Cisco SAN-OS Release 3.2(2c). Find the image release number you are currently using in the Current column of the table and use the path recommended.



Note

The software upgrade information in [Table 6](#) applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and SSM intelligent services traffic.



Caution

Upgrading from Cisco MDS SAN-OS Release 3.0(3) with SSI Release 3.0(3i) to SAN-OS Release 3.2(2c) with SSI Release 3.2(3k) will be disruptive.

Table 6 Nondisruptive Upgrade Path to SAN-OS Release 3.2(2c)

Current	Nondisruptive Upgrade Path
SAN-OS 3.2(1a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.1(4)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.1(3a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.1(2b)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.1(2a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.1(2)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.1(1)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.0(3a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.0(3)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.0(2a)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.0(2)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.0(1)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 2.1(3)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 2.1(2e)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 2.1(2d)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 2.1(2b)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).

Send documentation comments to mdsfeedback-doc@cisco.com

Table 6 ***Nondisruptive Upgrade Path to SAN-OS Release 3.2(2c) (continued)***

Current	Nondisruptive Upgrade Path
SAN-OS 2.1(2)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(2c).
SAN-OS 2.1(1b)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(2c).
SAN-OS 2.1(1a)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(2c).
SAN-OS 2.0(x)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.2(2c). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.2(2c).
SAN-OS 1.x	Upgrade to SAN-OS Release 1.3(4a), then to Release 2.1(2b), and then upgrade to Release 3.2(2c).

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

FICON Supported Releases and Upgrade Paths

Cisco MDS SAN-OS Release 3.2(2c) does support FICON.

[Table 7](#) lists the SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON upgrade path information.

Table 7 *FICON Supported Releases*

FICON Supported Releases	
NX-OS	Release 4.1(1c)
SAN-OS	Release 3.3(1c)
	Release 3.2(2c)
	Release 3.0(3b)
	Release 3.0(3)
	Release 3.0(2)
	Release 2.0(2b)

Use [Table 8](#) to determine your FICON nondisruptive upgrade path to Cisco MDS SAN-OS Release 3.2(2c). Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and use the path recommended.

Table 8 *FICON Nondisruptive Upgrade Path to SAN-OS 3.2(2c)*

Current Release with FICON Enabled	Upgrade Path
SAN-OS 3.0(3b)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 3.0(2)	You can nondisruptively upgrade directly to SAN-OS Release 3.2(2c).
SAN-OS 2.0(2b)	Use the interface shutdown command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively upgrading from SAN-OS Release 2.0(2b) to SAN-OS Release 3.0(2) or SAN-OS Release 3.0(3b), and then upgrade to Release 3.2(2c). An operationally down state includes Link failure or not-connected, SFP not present, or Error Disabled status in the output of a show interface command. When an interface is administratively shut it will then show as Administratively down. Interfaces that are currently up or trunking do not need to be shut down.
SAN-OS 1.x	Upgrade to SAN-OS Release 3.0(2). Use the interface shutdown command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively upgrading to Release 2.0(2b) and then upgrade to 1.3(4a).

Upgrading with IVR Enabled

An Inter-Switch Link (ISL) flap resulting in fabric segmentation or a merge during or after an upgrade from Cisco MDS SAN-OS Release 2.0(x) to a later image where IVR is enabled might be disruptive. Some possible scenarios include the following:

Send documentation comments to mdsfeedback-doc@cisco.com

- FCIP connection flapping during the upgrade process resulting in fabric segmentation or merge.
- ISL flap results in fabric segmentation or merge because of hardware issues or a software bug.
- ISL port becomes part of PCP results in fabric segmentation or merge because of a port flap.

If this problem occurs, syslogs indicate a failure and the flapped ISL could remain in a down state because of a domain overlap.

This issue was resolved in Cisco SAN-OS Release 2.1(2b); therefore, you must upgrade to Release 2.1(2b) before upgrading to Release 3.2(2c). An upgrade from Cisco SAN-OS Releases 2.1(1a), 2.1(1b), or 2.1(2a) to Release 2.1(2b) when IVR is enabled requires that you follow the procedure below, and then follow the upgrade guidelines listed in the [“Upgrading Your Version of Cisco Fabric Manager” section on page 13](#). If you have VSANs in interop mode 2 or 3, you must issue an IVR refresh for those VSANs.

To upgrade from Cisco SAN-OS Releases 2.1(1a), 2.1(1b), or 2.1(2a) to Release 2.1(2b) for all other VSANs with IVR enabled, follow these steps:

- Step 1** Configure static domains for all switches in all VSANs where IVR is enabled. Configure the static domain the same as the running domain so that there is no change in domain IDs. Make sure that all domains are unique across all of the IVR VSANs. We recommend this step as a best practice for IVR-non-NAT mode. Issue the **fcdomain domain id static vsan vsan id** command to configure the static domains.



Note Complete Step 1 for all switches before moving to Step 2.

- Step 2** Issue the **no ivr virtual-fcdomain-add vsan-ranges vsan-range** command to disable RDI mode on all IVR enabled switches. The range of values for a VSAN ID is 1 to 4093. This can cause traffic disruption.



Note Complete Step 2 for all IVR enabled switches before moving to Step 3.

- Step 3** Check the syslogs for any ISL that was isolated.

```
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED:
%$VSAN 2005%$ Isolation of interface
port-channel 52 (reason: unknown failure)
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED: %$VSAN 2005%$
Isolation of interface port-channel 51
(reason: domain ID assignment failure)
```

- Step 4** Issue the following commands for the isolated switches in Step 3:

```
switch(config)# vsan database
switch(config-vsan-db)# vsan vsan-id suspend
switch(config-vsan-db)# no vsan vsan-id suspend
```

- Step 5** Issue the **ivr refresh** command to perform an IVR refresh on all the IVR enabled switches.

- Step 6** Issue the **copy running-config startup-config** command to save the RDI mode in the startup configuration on all of the switches.

- Step 7** Follow the normal upgrade guidelines for Release 2.1(2b). If you are adding new switches running Cisco MDS SAN-OS Release 2.1(2b) or later, upgrade all of your existing switches to Cisco SAN-OS Release 2.1(2b) as described in this workaround. Then follow the normal upgrade guidelines for Release 3.2(2c).

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

RDI mode should not be disabled for VSANs running in interop mode 2 or interop mode 3.

Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2(2c)

Starting with Cisco MDS SAN-OS Release 3.0(1), the SSM front panel ports can no longer be configured in auto mode, which is the default for releases prior to Release 3.0(1).

**Note**

To avoid any traffic disruption, modify the configuration of the SSM ports as described below, before upgrading a SAN-OS software image prior to Release 3.2(2c).

For more information on upgrading SAN-OS software, see the [“Upgrading Your Cisco MDS SAN-OS Software Image”](#) section on page 12.

If the configuration is not updated before the upgrade, the installation process for the new image will automatically convert all ports configured in auto mode to Fx mode. This change in mode might cause a disruption if the port is currently operating in E mode.

To upgrade the image on your SSM without any traffic disruption, follow these steps:

Step 1 Verify the operational mode for each port on the SSM using the **show interface** command:

```
switch# show interface fc 2/1 - 32
fc2/1 is up
  Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
  Port WWN is 20:4b:00:0d:ec:09:3c:00
  Admin port mode is auto          <----- shows port is configured in auto mode
  snmp traps are enabled
  Port mode is F, FCID is 0xef0300 <----- shows current port operational mode is F
  Port vsan is 1
  Speed is 2 Gbps
  Transmit B2B Credit is 3
```

Step 2 Change the configuration for the first port of the quad when the admin port mode is auto. (A quad is a group of four ports, supported by a data path processor (DPP). The groups are 1 to 4, 5 to 8, 9 to 12, and so on.) Do not leave the port mode set to auto.

- a. Set the port admin mode to E or Fx if the current operational port mode is E, TE, F or FL.

```
switch# config t
switch(config)# interface fc 2/1
switch(config-if)# switchport mode fx
```

- b. Set the port admin mode to E if the current operational port mode is E:

```
switch# config t
switch(config)# interface fc 2/5
switch(config-if)# switchport mode e
```

Step 3 Change the configuration for ports 2, 3, and 4 of the quad:

- a. Set the admin port mode to Fx if the admin port mode of these ports is E, TE, or auto.

```
switch# config t
switch(config)# interface fc 2/2
switch(config-if)# switchport mode fx
```

Send documentation comments to mdsfeedback-doc@cisco.com

- b. If the first port in the port group has admin mode E or if the port is operational in E port mode, change the admin state of ports 2, 3, and 4 to shutdown.

```
switch# config t
switch(config)# interface fc 2/2
switch(config-if)# shutdown
```

- Step 4** Save the running configuration to the startup configuration before the upgrade procedure to ensure that the changes are preserved during and after the upgrade. To save the configuration, enter the following command:

```
switch# copy running-config startup-config
```

Upgrading the SSI Image on Your SSM

Use the following guidelines to nondisruptively upgrade the SSI image on your SSM:

- Install and configure dual supervisor modules.
- SSM intelligent services traffic on SSM ports is disrupted during upgrades. Fibre Channel switching traffic is not disrupted under the following conditions:
 - Upgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the [Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images](#).
 - All SSM applications are disabled. Use the **show ssm provisioning** CLI command to determine what applications are configured. Use the **no ssm enable feature** CLI command to disable these applications.
 - No SSM ports are in auto mode. See the “[Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2\(2c\)](#)” section on page 20.
 - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module slot epld** CLI command to determine your EPLD version. Refer to the [Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images](#) to upgrade your EPLD image.
 - Refer to the [Cisco MDS Storage Services Module Interoperability Support Matrix](#) and the “[Managing Modules](#)” chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x*, for information on upgrading your SSM.



Caution

Upgrading from Cisco MDS SAN-OS Release 2.1(1b) or earlier to Release 2.1.2 or later can disrupt traffic on any SSM installed on your MDS switch



Caution

Upgrading from Cisco MDS SAN-OS Release 3.0(3) with SSI Release 3.0(3i) to SAN-OS Release 3.2(2c) with SSI Release 3.2(3k) will be disruptive.

Upgrading a Switch with Insufficient Space for Two Images on the Bootflash

To upgrade the SAN-OS image on a Cisco MDS 9000 Family switch requires enough space on the internal CompactFlash (also referred to as bootflash) to accommodate both the old software image and the new software image.


Send documentation comments to mdsfeedback-doc@cisco.com

As of Cisco MDS SAN-OS Release 3.1(1), on MDS switches with a 256-MB CompactFlash, it is possible in some scenarios that a user might be unable to fit two images on the bootflash. This lack of space on the bootflash might cause the upgrade process to fail because new images are always copied onto the bootflash during an upgrade.

The following MDS switches are affected by this issue:

- MDS 9216 and MDS 9216i
- MDS 9120 and MDS 9140
- MDS 9500 Series switches with a Supervisor 1 module

To work around an image upgrade failure caused by a lack of space on the bootflash, follow these steps:

-
- Step 1** Prior to installing the new image, copy the old (existing) system image file to an external server. You may need to reinstall this file later.
- Step 2** Delete the old system image file from the bootflash by using either the Fabric Manager install utility or the CLI **delete bootflash:** command. The system image file does not contain the word “kickstart” in the filename.
- ```
switch# delete bootflash:m9200-ek9-mz.3.0.3.bin
```
- 
-  **Note** On MDS 9500 Series switches, you also need to delete the image file from the standby supervisor after deleting it from the active supervisor.
- ```
switch# delete bootflash://sup-standby/m9500-sf1ek9-mz.3.0.3.bin
```
-
- Step 3** Start the image upgrade or installation process using the Fabric Manager install utility or the CLI **install all** command.
- Step 4** If the new installation or upgrade fails while copying the image and you want to keep the old (existing) image, then copy the old image (that you saved to an external server in Step 1) to the bootflash using either Fabric Manager or the **copy** command.
- Step 5** If the switch fails to boot, then follow the recovery procedure described in the “Troubleshooting Installs, Upgrades, and Reboots” section of the [Cisco MDS 9000 Family Troubleshooting Guide, Release 3.x](#).
-

Upgrading a Cisco MDS 9124 Switch

If you are upgrading from Cisco MDS SAN-OS Release 3.1(1) to Cisco SAN-OS Release 3.2(2c) on a Cisco MDS 9124 Switch, follow these guidelines:

Send documentation comments to mdsfeedback-doc@cisco.com

- During the upgrade, configuration is not allowed and the fabric is expected to be stable.
- The Fabric Shortest Path First (FSPF) timers must be configured to the default value of 20 seconds; otherwise, the nondisruptive upgrade is blocked to ensure that the maximum down time for the control plane can be 80 seconds.
- If there are any CFS commits in the fabric, the nondisruptive upgrade will fail.
- If there is a zone server merge in progress in the fabric, the nondisruptive upgrade will fail.
- If a service terminates the nondisruptive upgrade, the **show install all failure-reason** command can display the reason that the nondisruptive upgrade cannot proceed.
- If there is not enough memory in the system to load the new images, the upgrade will be made disruptive due to insufficient resources and the user will be notified in the compatibility table.

Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch

Cisco MDS SAN-OS software upgrades are disruptive on the following single supervisor Cisco MDS Family switches:

- MDS 9120 switch
- MDS 9140 switch
- MDS 9216i switch

If you are performing an upgrade on one of those switches, you should follow the nondisruptive upgrade path shown in [Table 6](#), even though the upgrade is disruptive. Following the nondisruptive upgrade path ensures that the binary startup configuration remains intact.

If you do not follow the upgrade path, (for example, you upgrade directly from SAN-OS Release 2.1(2) or earlier version to SAN-OS Release 3.2(2c)), the binary startup configuration is deleted because it is not compatible with the new image, and the ASCII startup configuration file is applied when the switch comes up with the new upgraded image. When the ASCII startup configuration file is applied, there may be errors. Because of this, we recommend that you follow the nondisruptive upgrade path.

Downgrading Your Cisco MDS SAN-OS Software Image

This section lists the guidelines recommended for downgrading your Cisco MDS SAN-OS software image and contains the following sections:

- [General Downgrading Guidelines, page 23](#)
- [Downgrading the SSI Image on Your SSM, page 26](#)

General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.2(2c):

Send documentation comments to mdsfeedback-doc@cisco.com

- Install and configure dual supervisor modules.
- Issue the system **no acl-adjacency-sharing** execute command to disable acl adjacency usage on Generation 2 and Generation 1 modules. If this command fails, reduce the number of zones, IVR zones, TE ports, or a combination of these in the system and issue the command again.
- Disable all features not supported by the downgrade release. Use the **show incompatibility system downgrade-image** CLI command to determine what you need to disable.
- Layer 2 switching traffic is not disrupted when downgrading to Cisco SAN-OS Release 2.1(2) or later.
- Use the **show install all impact downgrade-image** CLI command to determine if your downgrade will be nondisruptive.
- Be aware that some features impact whether a downgrade is disruptive or nondisruptive:
 - **Fibre Channel Ports:** Traffic on Fibre Channel ports can be nondisruptively downgraded. See [Table 9](#) for the nondisruptive downgrade path for all SAN-OS releases.
 - **SSM:** Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during a downgrade. SSM Fibre Channel traffic is not.
 - **Gigabit Ethernet Ports:** Traffic on Gigabit Ethernet ports is disrupted during a downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module, the MSM-18/4 module, and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the downgrade is in progress.
 - **iSCSI:** If you are downgrading from SAN-OS version 3.0(x) to a lower version of SAN-OS, enable iSCSI if an IPS module, MPS-14/2 module, MSM-18/4 module, or the MDS 9222i switch is online. Otherwise, the downgrade will disrupt traffic.
 - **IVR:** With IVR enabled, you must follow additional steps if you are downgrading from Cisco SAN-OS Release 2.1.(1a), 2.1(1b), or 2.1.(2a). See the “[Upgrading with IVR Enabled](#)” section on [page 18](#) for these instructions.
 - **FICON:** If you have FICON enabled, the downgrade path is different. See [Table 10](#).
 - **iSNS:** The iSNS feature does not support a graceful downgrade from Cisco MDS SAN-OS Release 3.2(2c) to any earlier SAN-OS release. Prior to a downgrade from Cisco SAN-OS 3.2(2c), disable the MDS iSNS server and remove all configurations associated with the MDS iSNS client.

Use [Table 9](#) to determine your nondisruptive downgrade path from Cisco SAN-OS Release 3.2(2c). Find the SAN-OS image you want to downgrade to in the To SAN-OS Release column of the table and use the path recommended.



Note

The software downgrade information in [Table 9](#) applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and SSM intelligent services traffic.

Table 9 Nondisruptive Downgrade Path from SAN-OS Release 3.2(2c)

To SAN-OS Release	Nondisruptive Downgrade Path
SAN-OS 3.2(1a)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.1(4)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.1(3a)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).

Send documentation comments to mdsfeedback-doc@cisco.com

Table 9 Nondisruptive Downgrade Path from SAN-OS Release 3.2(2c)

To SAN-OS Release	Nondisruptive Downgrade Path
SAN-OS 3.1(2b)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.1	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.1(2)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.1(1)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.0(3a)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.0(3)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.0(2a)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.0(2)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.0(1)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 2.1(3)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 2.1(2e)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 2.1(2d)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 2.1(2b)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 2.1(2)	Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.1(2).
SAN-OS 2.1(1b)	Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.1(1b).
SAN-OS 2.1(1a)	Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.1(1a).
SAN-OS 2.0(4a)	Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(4a).
SAN-OS 2.0(4)	Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(4).
SAN-OS 2.0(3)	Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(3).
SAN-OS 2.0(2b)	Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(2b).
SAN-OS 2.0(1b)	Downgrade to SAN-OS Release 2.1(2b) and then downgrade to Release 2.0(1b).
SAN-OS 1.x	Downgrade to SAN-OS to Release 2.1(2b), then to Release 1.3(4a), and then downgrade to your SAN-OS 1.x release.

FICON Downgrade Paths

Cisco MDS NX-OS Release 3.2(2c) supports FICON.

Find the image release number that you want to downgrade to in the To SAN-OS Release with FICON Enabled column of [Table 10](#) and follow the recommended downgrade path.

Use [Table 10](#) to determine your nondisruptive downgrade path, if you have FICON enabled, from Cisco SAN-OS Release 3.2(2c). Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and use the path recommended.

Table 10 FICON Downgrade Path from SAN-OS 3.2(2c)

To SAN-OS Release with FICON Enabled	Downgrade Path
SAN-OS 3.0(3b)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).
SAN-OS 3.0(2)	You can nondisruptively downgrade directly from SAN-OS Release 3.2(2c).

Send documentation comments to mdsfeedback-doc@cisco.com

Table 10 *FICON Downgrade Path from SAN-OS 3.2(2c)*

To SAN-OS Release with FICON Enabled	Downgrade Path
SAN-OS 2.0(2b)	Use the interface shutdown command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively downgrading from SAN-OS Release 3.2(2c) to SAN-OS Release 3.0(3b) or SAN-OS Release 3.0(2), and then to SAN-OS Release 2.0(2b). An operationally down state includes <code>Link failure or not-connected</code> , <code>SFP not present</code> , or <code>Error Disabled</code> status in the output of a show interface command. When an interface is administratively shut it will then show as <code>Administratively down</code> . Interfaces that are currently up or trunking do not need to be shut down.
SAN-OS 1.3(4a)	Downgrade to SAN-OS Release 3.0(2). Use the shutdown command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively downgrading to Release 2.0(2b) and then downgrade to 1.3(4a).

Downgrading the SSI Image on Your SSM

Use the following guidelines when downgrading your SSI image on your SSM.

- On a system with at least one SSM installed, the **install all** command might fail on an SSM when you downgrade from Cisco SAN-OS Release 3.2(2c) to any SAN-OS 2.x release earlier than SAN-OS Release 2.1(2e). Power down the SSM and perform the downgrade. Bring up the SSM with the new bootvar set to the 2.x SSI image.
- Downgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the [Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images](#).
- SSM intelligent services traffic switching on SSM ports is disrupted on upgrades or downgrades.
- Fibre Channel switching traffic on SSM ports is not disrupted under the following conditions:
 - All SSM applications are disabled. Use the **show ssm provisioning** CLI command to determine if any applications are provisioned on the SSM. Use the **no ssm enable feature** configuration mode CLI command to disable these features.
 - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module slot epld** CLI command to determine your EPLD version. Refer to the [Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images](#) to upgrade your EPLD image.
 - Refer to the [Cisco MDS Storage Services Module Interoperability Support Matrix](#) and to the “Managing Modules” chapter in the [Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x](#) for information on downgrading your SSM.

New Features in Cisco MDS SAN-OS Release 3.2(2c)

This section briefly describes the new features introduced in this release. For detailed information about the features listed, refer to the [Cisco MDS 9000 Family CLI Configuration Guide](#), the [Cisco MDS 9000 Family Fabric Manager Configuration Guide](#), and the [Cisco MDS 9000 Family Storage Media Encryption Configuration Guide](#). For information about new CLI commands associated with these

Send documentation comments to mdsfeedback-doc@cisco.com

features, refer to the [Cisco MDS 9000 Family Command Reference](#). The “New and Changed Information” section in each of these books provides a detailed list of all new features and includes links to the feature description or new command.

Cisco Storage Media Encryption

Cisco Storage Media Encryption (SME) for the Cisco MDS 9000 family switches offers a highly scalable, reliable, and flexible solution to encrypting sensitive information in the data center. SME is integrated transparently as a fabric service for Fibre Channel SANs. It is a complete solution and offers the following features:

- Strong AES-256 encryption of data at rest
- Heterogeneous device support: tape drives, virtual tape libraries (VTL)
- Seamless integration as a transparent fabric service
- Nondisruptive installation and provisioning
- High availability and scalability
- Secure, comprehensive key management
- Full role-based access control support for management
- Provisioning and key management integrated with Cisco Fabric Manager and CLI

Cisco SME secures data stored on the heterogeneous tapes in a SAN environment using Advanced Encryption Standard (AES) 256-bit algorithm. Cisco SME capabilities are provided as a fabric service, rather than on a separate hardware appliance like the leading competitors provide. Traffic between any host and disk on the fabric can use the Cisco SME services.

N-Port Identifier Virtualization Support for Cisco MDS 9124 and 9134 Switches

N-Port Identifier Virtualization (NPIV) support for Cisco MDS 9124 and 9134 fabric switches is included in this release.

NPIV Requirements

[Table 11](#) shows the minimum SAN-OS releases that support NPIV.

Table 11 NPIV Core SAN-OS Requirements

Switch	Minimum SAN-OS Release
MDS 9124, MDS 9134	Release 3.2(2c)
MDS 9200, MDS 9500	Release 3.2(1)

NPIV is not supported on the MDS 9020 switch and the MDS 9040 switch.



Note

Upgrades from any of the versions listed in the table above with NPIV enabled will be non-disruptive. If you have not yet enabled NPIV and you are planning to enable NPIV, you should upgrade to one of the versions listed above or later before enabling NPIV.

Send documentation comments to mdsfeedback-doc@cisco.com

**Note**

When upgrading from Release 3.2(1x) or an earlier release, to Release 3.2(2x) or later on an MDS 9124 or MDS 9134 switch with NPIV enabled, you must disable NPIV before upgrading for a non-disruptive upgrade. This will limit the disruption to ports already logged in using NPIV; other traffic will not be affected. With NPIV turned on, the upgrade will be disruptive.

New MIBS

The following new MIB is included in Cisco MDS 9000 SAN-OS release 3.2(2c):

- CISCO-SME-MIB

MDS Authentication Mode

As of SAN-OS Release 3.x, Cisco Fabric Manager required users to log in to the Fabric Manager server and the switches in the fabrics. This resulted in a two-step login process. The MDS authentication mode option has been added to the Cisco Fabric Manager installer to enable users to log in to the Fabric Manager server with switch credentials, restoring the one-step login process. This feature can be used with both the standalone and Fabric Manager Server configurations.

If more than one fabric is going to be opened by Cisco Fabric Manager in the MDS authentication mode, both switch fabrics must have the same credentials for a user.

Changes in Existing Features

iSNS

As of Cisco SAN-OS Release 3.2(2c), iSNS server and iSNS client features are deprecated.

Send documentation comments to mdsfeedback-doc@cisco.com

Limitations and Restrictions

This section lists the limitations and restrictions for this release. This section includes the following topics:

- [Upgrading to Recover Loss of Performance Manager Data, page 29](#)
- [Java Web Start, page 30](#)
- [Cisco SME Configuration Limits, page 30](#)
- [Deprecated iSCSI Features, page 30](#)
- [Data Mobility Manager, page 31](#)
- [Compatibility of Fabric Manager and Data Mobility Manager, page 31](#)
- [Cisco MDS 9134 Multilayer Fabric Switch, page 31](#)
- [Cisco MDS 9222i Multiservice Modular Switch and Cisco MDS 9000 18/4-Port Multiservice Module, page 32](#)
- [Using SAN Device Virtualization on Cisco Fabric Switches, page 32](#)
- [CWDM SFPs, page 33](#)
- [Fabric Manager, page 33](#)
- [MTU Size Limitation, page 33](#)
- [Reconfiguring SSM Ports, page 33](#)
- [Virtual Router Redundancy Protocol \(VRRP\) Interfaces, page 33](#)
- [QoS on an MDS 48-port Fibre Channel Module, page 34](#)
- [Maximum Number of Zones Supported in Interop Mode 4, page 34](#)
- [Configuring Default Settings for the Default Zone, page 34](#)
- [PPRC Not Supported with FCIP Write Acceleration, page 34](#)
- [Using IVR In a Fabric With Mixed Code Versions, page 34](#)

Upgrading to Recover Loss of Performance Manager Data



Caution

You must upgrade to Fabric Manager Release 3.1(x) and then upgrade to a later release of Fabric Manager to avoid losing Performance Manager data. If data has been lost, follow the steps below to recover the data.

-
- Step 1** Disable Performance Manager interpolation using Fabric Manager Web Client. Uncheck **Interpolate missing statistics**, then click **Apply**.
 - Step 2** Stop the Fabric Manager Server.
 - Step 3** Save the data file in the `$INSTALL_DIR` directory.
 - Step 4** Move the old RRD file into the `$INSTALL_DIR/pm/db` directory.
 - Step 5** Run `$INSTALL_DIR/bin/pm.bat m`.

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

Step 6 Restart Fabric Manager Server.

Java Web Start

When using Java Web Start, it is recommended that you do not use an HTML cache or proxy server. You can use the Java Web Start Preferences panel to view or edit the proxy configuration. To do this, launch the Application Manager, either by clicking the desktop icon (Microsoft Windows), or type **./javaws** in the Java Web Start installation directory (Solaris Operating Environment and Linux), and then select **Edit>Preferences**.

If you fail to change these settings, you may encounter installation issues regarding a version mismatch. If this occurs, you should clear your Java cache and retry.

Cisco SME Configuration Limits

Table 12 lists the Cisco SME configuration limits for this release.

Table 12 *Cisco SME Limits*

Configuration	Limit
Number of clusters per switch	1
Switches in a cluster	4
Fabrics in a cluster	1
Modules in a switch	11
Cisco MSM-18/4 modules in a cluster	32
Initiator-Target-LUNs (ITLs)	128
LUNs behind a target	32
Host and target ports in a cluster	128
Number of hosts per target	8
Tape backup groups per cluster	2
Volume groups in a tape backup group	4
Cisco Key Management Center (# of keys)	32K
Targets per switch that can be FC-redirected	32

Deprecated iSCSI Features

The following iSCSI features are no longer supported in Cisco MDS 9000 SAN-OS release 3.2(1):

- iSNS server or iSNS client
- Trespass feature
- Pass-through and cut-through modes (only iSCSI CRC with store and forward is supported)
- iSCSI interface specific TMF queuing option (perform TMF queuing by default)

Send documentation comments to mdsfeedback-doc@cisco.com

Data Mobility Manager

Use the following guidelines when running Cisco Data Mobility Manager (DMM):

- If you have a DMM configuration, the DMM job may transition to a Reset state during a supervisor switchover. In that case, the administrator should recover from the Reset state by following the instructions in the *Cisco MDS 9000 Data Mobility Manager Configuration Guide*.
- A storage type job in DMM cannot be restored from a saved ASCII configuration. When a storage job is created in DMM, the SSM generates Virtual Initiators (VIs) for each storage type job. Each request to generate VIs can potentially return different VI pWWNs. As a result, if an ASCII configuration for a storage type job is reapplied, there is a possibility the VIs generated by the SSM are different. In that case, the session configurations in the saved configuration are no longer valid.
- Following a **fcdomain restart disruptive** command, the DMM process cleans up all configurations and transitions the DMM job in the affected VSAN to the Reset state. During the cleanup, some virtual devices are not deleted correctly, which results in an incomplete cleanup. As a result, when the administrator validates the DMM job from the CLI or restarts or schedules the DMM job from Fabric Manager, the operation fails. If this situation occurs with a DMM job configured on the SSM, then reload the SSM to recover the DMM job.
- For active-passive arrays, DMM requires that the administrator create two DMM jobs: one for the active LUNs from one controller and the other for the active LUNs on the other controller. DMM provides the Server Lunmap Discovery (SLD) tool to detect if the array is in fact active-passive. On the IBM DS-4500 storage device, the SLD cannot successfully detect active-passive LUNs on a storage port. As a consequence, the administrator will have to determine which LUNs are active on which port and create DMM jobs accordingly.
- A DMM job that is in progress might fail if you change the clock on an MDS switch by configuring the NTP server.

Compatibility of Fabric Manager and Data Mobility Manager

Cisco Fabric Manager in any MDS NX-OS 4.1(x) release does not support Data Mobility Manager (DMM) in any SAN-OS 3.3(x) release or in any 3.2(x) release. To use the Cisco Fabric Manager GUI for DMM, both Fabric Manager and DMM must be running NX-OS or SAN-OS software from the same release series.

Cisco MDS 9134 Multilayer Fabric Switch

The Cisco MDS 9134 Multilayer Fabric Switch does not support the following Cisco MDS SAN-OS features:

- IVR
- Remote SPAN
- Translative loop support
- FCC—No generation, quench reaction only

In addition, the following features have these limits:

- VSANs—16 maximum
- SPAN—1 session maximum

Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9222i Multiservice Modular Switch and Cisco MDS 9000 18/4-Port Multiservice Module

The Cisco MDS 9222i Multiservice Modular Switch and the Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) support one iSCSI forwarding mode that is equivalent to store-forward on the MPS-14/2 module.

The Cisco MDS 9222i switch and the MSM-18/4 module support header-digest, but not data-digest in Cisco SAN-OS 3.2(2c).

The Cisco MDS 9222i switch and the MSM-18/4 module do not support Ether channel.

The Cisco MDS 9222i switch supports only the following modules in slot 2:

- The Storage Services Module (SSM)
- The Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4)
- The 8-port Gigabit Ethernet IP Storage services module
- The MDS 9000 12-, 24-, and 48-port 4-Gbps Fibre Channel modules
- The MDS 9000 4-port 10-Gbps Fibre Channel module

The MSM-18/4 module and MDS 9222i switch do not support the following features:

- Special frames for FCIP
- B ports for San Extension
- SAN extension tuner
- NetSim
- IPv6
- FCIP between the MSM-18/4 module and another IPS module

Using SAN Device Virtualization on Cisco Fabric Switches

There must be at least one SAN device virtualization-enabled switch that is not a Cisco MDS 9124 switch, a Cisco Fabric Switch for HP c-Class BladeSystem, or a Cisco Fabric Switch for IBM BladeCenter between the server and the target that are being virtualized. In other words, SAN device virtualization does not work when initiators and primary targets are connected to the same Cisco MDS 9124 Switch or or Cisco MDS 9134 Switch or Cisco Fabric Switch for HP c-Class BladeSystem or Cisco Fabric Switch for IBM BladeCenter.

Send documentation comments to mdsfeedback-doc@cisco.com

CWDM SFPs

The 2-Gbps CWDM SFPs do not have a maximum speed set in memory and they negotiate to 4-Gbps on modules that support the higher speed. As a result, the link comes up and appears to work, but then becomes disabled and connectivity problems occur. To correct this problem, both sides of the connection must have their speed hard coded to 2-Gbps.

Fabric Manager

Observe the following limitations or restrictions for the Cisco SAN-OS Release 3.2(2c) for Fabric Manager:

- By default, the database and aaa passwords are stored in plain text. You can encrypt them by using the `encrypt.bat/.sh` script and pasting the output into the appropriate file, either `server.properties` or `aaa.properties`.
- The Microsoft Security Patch MS06-040 is known to break applications with a large heap memory. If you increase any Java application's heap (including Fabric Manager) beyond 64 M, we recommend you do not apply this patch.
- If port 80 on the switch is blocked and you are using VPN, Fabric Manager cannot detect NAT addresses. The timeout for URL connections is set for 500ms.

MTU Size Limitation

The Cisco MDS 9216i switch and MPS-14/2 module do not support an MTU size greater than 8000 bytes. An attempt to set the MTU size greater than 8000 bytes will result in an error. As a workaround, reset the value of the MTU size (576 to 8000 bytes) and issue the `no shutdown` command on the interface for normal operation.

Reconfiguring SSM Ports

Starting with Cisco MDS SAN-OS Release 3.0(1), the SSM front panel ports can no longer be configured in auto mode, which is the default for releases prior to Release 3.1(1). For instructions about how to modify the configuration of the ports before upgrading to SAN-OS Release 3.1(3a), see the [“Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.2\(2c\)”](#) section on page 20.

Virtual Router Redundancy Protocol (VRRP) Interfaces

When a switchover occurs on a switch that is the master for Virtual Router Redundancy Protocol (VRRP) interfaces, the switchover may cause a minor delay. As a result, the VRRP backup (occurring elsewhere) may assume the role of the VRRP master. As a workaround, increase the VRRP advertisement interval for these interfaces.

Send documentation comments to mdsfeedback-doc@cisco.com

QoS on an MDS 48-port Fibre Channel Module

Due to possible differences in parts per million between the MAC ASICs on both sides of an ISL link, there is a potential throughput issue when running QoS over an ISL on an MDS 48-port Fibre Channel module. Specifically, the user may not see traffic throughput that follows the programmed QoS ratios. The throughput ratio on the high and/or medium priority class of service (COS) relative to the low priority COS, may not be as high as the actual programmed ratio.

If this situation occurs, you can move the ISL to a port on a different port group on one and/or both sides of the link, or move the ISL to a port on a lower-density card if you require accurate QoS ratios.

Maximum Number of Zones Supported in Interop Mode 4

In interop mode 4, the maximum number of zones that is supported in an active zone set is 2047, due to limitations in the connected vendor switch.

When IVR is used in interop mode 4, the maximum number of zones supported, including IVR zones, in the active zone set is 2047.

Configuring Default Settings for the Default Zone

Following an upgrade from any Cisco SAN-OS 2.x release to any Cisco SAN-OS 3.x release, the configuration defined by the **zone default-zone permit vsan vsan-id** command is applied only to the active VSAN. The configuration does not apply to unconfigured VSANs. In SAN-OS 3.x, you can apply the configuration to unconfigured VSANs by issuing the **system default zone default-zone permit** command.

Similarly, the **zoneset distribute full vsan vsan-id** command applies only to the active VSAN following an upgrade from any Cisco SAN-OS 2.x release to any Cisco SAN-OS 3.x release.

Although you can configure the default-zone settings in the setup script, these settings do not take effect for VSAN 1, because VSAN 1 already exists prior to running the setup script. To configure the default settings for the default-zone in VSAN 1, you must explicitly enter the **zone default-zone permit** command.

PPRC Not Supported with FCIP Write Acceleration

IBM Peer to Peer Remote Copy (PPRC) is not supported with FCIP Write Acceleration.

Using IVR In a Fabric With Mixed Code Versions

If you are using IVR and you are running SAN-OS 3.x software on your MDS switches, make sure that all IVR switches run the same code version. Otherwise, if you have a fabric with mixed code versions, the switches running the higher version may not be able to see all IVR devices. The mixed fabric can cause an inconsistent database among IVR switches, which might affect IVR behavior. For this reason, it is important that all IVR switches run the same SAN-OS version, preferably SAN-OS Release 3.3(4a), which has device update (DU) support, or later.

Send documentation comments to mdsfeedback-doc@cisco.com

Caveats

This section lists the open and resolved caveats for this release. Use [Table 13](#) to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

Table 13 *Open Caveats and Resolved Caveats Reference*

DDTS Number	Software Release (Open or Resolved)	
	3.2(1a)	3.2(2c)
Severity 2		
CSCsg49151	O	O
CSCsi72048	O	O
CSCsk22374	O	R
CSCsk31869	O	R
CSCsk43922	O	O
CSCsk49029	O	O
CSCsk49634	O	O
CSCsk49761	O	O
CSCsk51193	O	O
CSCsk58368	O	R
CSCsk71439	O	R
CSCsk73484	O	R
CSCsk78735	O	R
CSCsk86748	O	R
CSCsl04943	O	R
CSCsl16409	O	R
CSCsl53091	—	O
CSCsl72080	—	O
CSCso72230	O	O
Severity 3		
CSCin95789	O	O
CSCse31881	O	O
CSCse47687	O	O
CSCsg19148	O	O
CSCsg19303	O	O
CSCsh70425	O	R
CSCsi66310	O	O
CSCsj24904	O	O
CSCsj32048	O	R

Send documentation comments to mdsfeedback-doc@cisco.com

Table 13 ***Open Caveats and Resolved Caveats Reference (continued)***

DDTS Number	Software Release (Open or Resolved)	
	3.2(1a)	3.2(2c)
CSCsj72666	O	O
CSCsk00953	O	R
CSCsk06186	O	O
CSCsk18352	O	R
CSCsk26424	O	R
CSCsk35725	O	O
CSCsk35951	O	O
CSCsk49309	O	O
CSCsk63929	O	O
CSCsk64172	O	R
CSCsk73370	O	R
CSCsk87502	O	O
CSCsk87614	O	O
CSCsk88049	O	R
CSCsk88959	O	R
CSCsk88967	O	R
CSCsk89586	O	R
CSCsk90564	O	R
CSCsk93682	O	R
CSCsk93834	O	O
CSCsk94090	O	R
CSCsk95241	O	O
CSCsk95464	O	R
CSCsk96105	O	R
CSCsl04532	—	O
CSCsl12130	O	O
CSCsl12611	—	O
CSCsl15511	O	O
CSCsl17944	O	O
CSCsl25170	O	R
CSCsl31087	—	O
CSCsl33763	—	O
CSCsl25170	O	R
CSCsl34922	—	O

Send documentation comments to mdsfeedback-doc@cisco.com

Table 13 **Open Caveats and Resolved Caveats Reference (continued)**

DDTS Number	Software Release (Open or Resolved)	
	3.2(1a)	3.2(2c)
CSCsm54598	—	O
CSCso63465	O	O
Severity 4		
CSCsi56167	O	O
CSCsk91974	O	O
Severity 5		
CSCsk73654	O	O
Severity 6		
CSCsk43927	O	O

Resolved Caveats

- [CSCsk22374](#)

Symptom: Some switching modules may reload after an upgrade to SAN-OS Release 3.0(1) through Release 3.2(1a). This issue is seen only on the MDS 12-port, 24-port, and 48-port 4-Gbps Fibre Channel switching modules, and on the 4-port 10-Gbps Fibre Channel switching module. It occurs after code has been downloaded to the module.

Workaround: This issue is resolved.

- [CSCsk31869](#)

Symptom: An IVR zone set activation or deactivation fails in a large topology. This occurs if an IVR fabric merge has failed and IVR queries CFS for a list of peer switches; however, CFS does not return the complete list of peers. IVR waits indefinitely for some of the peers to respond, which causes the IVR activation or deactivation to fail. This issue is seen only in very large topologies (for example, 75 switches).

Workaround: This issue is resolved.

- [CSCsk58368](#)

Symptom: During an in-service switch upgrade (ISSU) of a switch with an MDS-18/4 module, IVR is initialized later than the Fibre Channel name service (FCNS). FCNS checks with IVR for entries that it has in its persistent storage service (PSS) and that belong to IVR (for virtual domains). Since IVR is not initialized, it will not respond to FCNS. Because of this, an end device may not be advertised to transient VSANs or may not be visible to the IVR end device in a target VSAN.

Workaround: This issue is resolved.

- [CSCsk71439](#)

Symptom: Fabric Manager installation may fail with a messaging and transaction service (MTS) error message.

Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsk73484

Symptom: When changing from Layer2 to Layer3 mode using the **install ssi modflash:xxx module x12-upgrade** command, a test is run that may detect a parity error. If a parity error is detected, then an attempt to clear the parity error occurs. If the parity error is cleared then the install proceeds otherwise, the installation fails.

Workaround: This issue is resolved.

- CSCsk78735

Symptom: The fabric binding database has duplicate local entries.

Workaround: This issue is resolved.

- CSCsk86748

Symptom: In rare circumstances, a Cisco MDS 9000 Supervisor may unexpectedly reload. This can trigger a Supervisor switchover, or a complete switch reload in the case of non-HA platforms. After this event, the output of the **show system-reset reason** command will show output similar to following:

```
switch#show system reset-reason
----- reset reason for module 6 from local-supervisor -----
1) At 911546 usecs after Tue Oct 9 11:35:28 2007
    Reason: Reset triggered due to bad backplane communication channel
    Service: Failure Rx map 0x1f
    Version: 3.0(2a)
```

This issue occurs only in conditions of excessive Fibre Channel control path traffic. This is rare, but it can happen if, for example, multiple devices that are connected to the switch are reloaded at the same time.

Workaround: This issue is resolved.

- CSCsl04943

Symptom: The syslogs log file cannot be displayed because the **/tmp** directory is full. This occurs when the **Control - C** command is used to abort the **show logging logfile** dialog. When the **/tmp** directory is full, it can impact SAN-OS operations.

Workaround: This issue is resolved.

- CSCsl16409

Symptom: A CFS incompatibility exists between switches running SAN-OS Release 3.0.x and Release 3.1.x and switches running Release 3.2.1. In fabrics that include a mix of these SAN-OS versions, CFS on the switches running Release 3.0.x or Release 3.1.x may not see a switch running Release 3.2.1 as a CFS peer. SAN-OS Release 3.2.1 is not CFS-compatible with Release 3.0.x and Release 3.1.x. All other version combinations are compatible.

This could manifest in the following ways:

- CFS applications on switches running Release 3.0.x or Release 3.1.x may not merge with their peers on a switch running Release 3.2.1.
- Distributions initiated from switches running Release 3.0.x or Release 3.1.x will not make it to a switch running Release 3.2.1.

This incompatibility does not always occur; however, it occurs when:

- Switches running Release 3.2.1 host virtual domains.
- The domain ID of the real domain on a switch running Release 3.2.1 is less than that of the virtual domain it hosts.

Send documentation comments to mdsfeedback-doc@cisco.com

To identify if this issue occurs, issue the **show cfs merge status name <app-id>** command on switches running Release 3.2.1 to show the switches running Release 3.2.1 and the switches running Release 3.0.x and Release 3.1.x. Issue the **show cfs merge status name <app-id>** command on switches running Release 3.0x and Release 3.1.x to show only switches running Release 3.0.x and Release 3.1.x.

Workaround: This issue is resolved.

- CSCsk95464

Symptom: When a server HBA port is flapped multiple times, the storage-based migration job moves to the Reset state.

Workaround: This issue is resolved.

- CSCsk96105

Symptom: If you upgrade to Cisco SAN-OS Release 3.2(2c) from a lower version, or downgrade from Cisco SAN-OS Release 3.2(2c) to a lower version on an MDS 9124 switch, MDS 9134 switch, Cisco Fabric Switch for HP c-Class BladeSystem, or a Cisco Fabric Switch for IBM BladeCenter, zoning may not work as configured for the F ports connected to NPIV-capable hosts.

Workaround: This issue is resolved.

- CSCsl25170

Symptom: On a switch running SAN-OS Release 3.2(1), Release 3.2(1a) or Release 3.2(2a) with 2 or more MDS-18/4 modules present, when upgrading to SAN-OS Release 3.2(2c) or later, only the first MDS-18/4 module will be upgraded. The other MDS-18/4 modules will not be upgraded. They will continue to run the older release.

Workaround: This issue is resolved.

- CSCsl34881

Symptom: During a login to an MDS 9200 Family switch or an MDS 9134 switch, Performance Manager incorrectly displays the Request Node ID (RNID) when FICON is enabled.

Workaround: This issue is resolved.

- CSCsh70425

Symptom: The administrator can configure a data migration job to be in the offline mode in one fabric and in the online mode in another fabric.

Workaround: This issue is resolved.

- CSCsj32048

Symptom: T10K tape drives are not supported for FICON tape acceleration as remote tape drives behind the Sun StorageTek Virtual Storage Manager (VSM).

Workaround: This issue is resolved.

- CSCsk00953

Symptom: HP Blade Servers that are connected through an HP Virtual Connect (VC) FC module to a Cisco Fabric Switch for HP c-Class BladeSystem using NPIV lose access to LUNs when load balancing on the VC module is switched from 16:1 to 8:1. When the load balancing ratio is 16:1, all servers connect through interface ext1. When the ratio is 8:1, servers 1 and 3 connect through ext1, servers 2 and 4 connect through ext2, and so on. Servers on ext2 are not affected by the switchover. In addition, packets might get dropped when the switchover occurs.

Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsk18352
Symptom: If a supervisor switchover occurs while Fabric Manager is creating a DMM migration job, the job creation process times out.
Workaround: This issue is resolved.
- CSCsk26424
Symptom: Removing a fabric and then adding the same fabric in Fabric Manager causes a session fabric ID mismatch. As a result, hosts do not appear in the Step 1 window of the Fabric Manager DMM job creation wizard.
Workaround: This issue is resolved.
- CSCsk64172
Symptom: CFS does not successfully merge records from the persistent storage service (PSS) pertaining to the data portion of events. This results in a PSS leak and a memory leak where a large number of records in PSS cause long read and write access times.
Workaround: This issue is resolved.
- CSCsk73370
Symptom: In SAN-OS Release 3.2(1), the user configuration is not restored after a reload.
Workaround: This issue is resolved.
- CSCsk88049
Symptom: When using NASB with the EMC Clariion Disk Library (CDL), after enabling or disabling NASB (that is in the same VSAN as the CDL) multiple times, a login to the CDL from the NASB initiator can fail.
Workaround: This issue is resolved.
- CSCsk88959
Symptom: While an interface is shutdown, a zone might fail. The failure can occur when the **shutdown** and **no shutdown** commands are entered several times on the interface if the members of the zone are interface, fWWN, domain port, domain interface, device alias, symbolic node name, and IP address, and the members are present in an active zone set.
Workaround: This issue is resolved.
- CSCsk88967
Symptom: When installing Fabric Manager, servers using the password authentication method only fail the verification test. This occurs when you click **Verify Remote Server** during installation to test for connectivity. Fabric Manager supported only the keyboard interactive authentication method for SSH. Fabric Manager now supports password authentication also.
Workaround: This issue is resolved.
- CSCsk89586
Symptom: On the MDS 12-port, 24-port, and 48-port 4-Gbps Fibre Channel switching modules, and on the 4-port 10-Gbps Fibre Channel switching module, in SAN-OS Release 3.2(1) and older releases, if NPIV is enabled and the switch has been reloaded, the installer will not prevent an upgrade to Release 3.2(2c). After the upgrade, zoning may not work properly for the F-ports connected to NPIV capable hosts.
Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsk90564
Symptom: In large fabrics, an IVR activation or deactivation fails due to a Cisco Fabric Service (CFS)-Messaging and Transaction Service (MTS) reject.
Workaround: This issue is resolved.
- CSCsk93682
Symptom: If you upgrade to Cisco SAN-OS Release 3.2(2c) from a lower version, or downgrade from Cisco SAN-OS Release 3.2(2c) to a lower version on an MDS 9124 switch, MDS 9134 switch, Cisco Fabric Switch for HP c-Class BladeSystem, or a Cisco Fabric Switch for IBM BladeCenter, zoning may not work as configured for the F ports connected to NPIV-capable hosts.
Workaround: This issue is resolved.
- CSCsk94090
Symptom: When installing a Fabric Manager license, the Product Authorization Key (PAK) installation fails. This occurs when the VDH= string is no longer needed as part of the Cisco license server URL.
Workaround: This issue is resolved.

Open Caveats

- CSCsg49151
Symptom: If you bring up more than one link at a time between two VSANs that have overlapping domains and at least one of the switches is SDV enabled, one link will become isolated. The other links will come up, even though the domains are overlapping. In addition, the SDV virtual domains will change, causing traffic disruption on all devices associated with their old value.
Workaround: Bring up multiple links between two switches one at a time. Verify that the first link came up correctly before attempting to bring up the next link. If the first link fails to come up because of a domain ID overlap, resolve the domain conflict and then try again to bring up the links.
- CSCsi72048
Symptom: FCIP links may fail on an MDS 9216i switch that has compression set to auto when the other end of the FCIP link is terminated by an IPS-8 module. You may see the following message in the logs:

```
%IPS_SB_MGR-SLOT1-3-CRYPTO_FAILURE: Heartbeat failure in encryption engine (error 0x1)
%ETHPORT-5-IF_DOWN_SOFTWARE_FAILURE: Interface GigabitEthernet1/1 is down (Port software failure)
%PORT-5-IF_DOWN_SOFTWARE_FAILURE: %$VSAN 1$ Interface fcip99 is down (Port software failure)
```

Workaround: If both ends of an FCIP link are not on an MPS-14/2 module, do not use mode 1 and auto.
- CSCsk43922
Symptom: A data path processor (DPP) might fail on an MDS switch running SSI Release 3.2(1) on the SSM. The failure occurs after several days of running traffic when a misbehaving target sends unexpected frames well after the response has already been received from the same target.
Workaround: None.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsk49029

Symptom: If there is a request to export a domain while the same domain is being cleaned up, domain entries might not be programmed. As a result, communication between IVR devices might not occur.

Workaround: Because the the programming request was lost, the only way to retrigger the programming is to withdraw the domain and refresh IVR. Follow these steps:

1. Identify domains with problem using the **show ivr internal dep** command.

```
switch# show ivr internal dep
Internal information for DEP FSM
-----

vsan domain nh status sync_status req i/f
101 0x61(97) 1001 ALL_DONE OXID|FCID_RW 0 [ fc3/2 ]
102 0x62(98) 1002 ALL_DONE OXID|FCID_RW 0 [ fc3/5 ]
1001 0x9e(158) 101 NONE OXID|FCID_RW 0 [ fc2/16 ]
1002 0x98(152) 102 ALL_DONE OXID|FCID_RW 0 [ fc9/10]
Number of DEP entries : 4
```

After waiting for a few minutes for IVR to stabilize, if the status column for the {vsan, domain} combination is NONE, then this problem has occurred the switch.

2. Withdraw the troubled domains using the **ivr withdraw domain domain vsan vsan-id** command.
3. Readvertise the withdrawn domains using the **ivr refresh** command.

- CSCsk49634

Symptom: In rare cases, an FCIP link might flap on a network with high latency and a consistently high loss rate (above 100ms RTT and 0.5% loss).

Workaround: None.

- CSCsk49761

Symptom: When IVR exports a new virtual domain and multiple border switches export that virtual domain, some of the entries in the Fibre Channel name server (FCNS) database that correspond to this virtual domain may have partial entries where the port type contains a dash (-). This can then lead to a lack of IVR communication between these devices and other IVR devices.

Workaround: Use the **show ivr internal vdri vsan vsan-id domain domain** command to determine which border switch is exporting the virtual domain. Then on any of the border switches that is exporting the virtual domain, enter the following command for each device that has a partial FCNS entry:

```
switch(config)# ivr device pwwn pwwn fcns register vsan vsan-id
```

In this example, pWWN is the port pWWN of the device and vsan-id is the VSAN that contains the incomplete FCNS entries.

- CSCsk51193

Symptom: Following an upgrade to Cisco MDS SAN-OS Release 3.2(1) on a Cisco MDS 9124 switch, an interface is shown as up, but there is no FLOGI information for the port in the FLOGI database.

Workaround: Set the port mode to F.

CSCsl53091

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsl53091

Symptom: Issuing the **no-shut TL port** command to bring up a TL port on SANOS releases 3.2(2x) fails. The TL port remains in the init state.

Also, in Release 3.2(2x), if a Fibre Channel loop connected to an FL port does an LIP_F7 while the port is already in the Up state, the FL port will be reinitiated even if the LIP_F7 is supposed to be non-disruptive.

Workaround: None.

- CSCsl72080

Symptom: ISLB zone set activation and zone set distribute fails. The reason is shown as "Duplicate Member". This issue occurs in the following conditions:

- (i) When an active zone set is present in a VSAN and an ISLB zoneset activation is attempted.
- (ii) When zone set distribution is attempted in an IVR VSAN from Exec mode.

In SAN-OS Release 3.2.2 and Release 3.2.2x, the ISLB zone set activation and zone set distribution in an IVR VSAN are rejected by the zone server when an active zone set is present in a VSAN. The Duplicate Member message is displayed due to an incorrect validation. This issue has been resolved in SAN-OS Release 3.2.3 and later.

Workaround: For condition (i), there is no workaround. For condition (ii), full zone set distribution can be turned on for the IVR VSAN and when zone set activation is attempted, the complete zone database is distributed for that VSAN.

- CSCso72230

Symptom: In rare instances, the following Generation 2 modules might reload:

- 12-port 4-Gbps Fibre Channel module
- 24-port 4-Gbps Fibre Channel module
- 48-port 4-Gbps Fibre Channel module
- 4-port 10-Gbps Fibre Channel module

The output of the **show logging log** command will have events like those shown below. In the following output, module 7 is the supervisor and module 12 is the module that reloaded.

```
2008 Jul 15 19:39:30 fcd95c41 %MODULE-4-MOD_WARNING: Module 7 (serial: JAE1134UR88)
reported warnings on ports 7/1-7/3 (Unknown) due to BE2 Arbiter experienced an error
in device 65 (device error 0xc410d613)
2008 Jul 15 19:39:30 fcd95c41 %MODULE-4-MOD_WARNING: Module 8 (serial: JAE1134UOTD)
reported warnings on ports 8/1-8/3 (Unknown) due to BE2 Arbiter experienced an error
in device 65 (device error 0xc410d613)
2008 Jul 15 19:39:35 fcd95c41 %XBAR-5-XBAR_STATUS_REPORT: Module 12 reported status
for component 88 code 0x40240015.
2008 Jul 15 19:39:35 fcd95c41 %MODULE-2-MOD_DIAG_FAIL: Module 12 (serial: JAE1136VU6L)
reported failure on ports 12/1-12/24 (Fibre Channel) due to Fatal runtime Arb error.
(DevErr is bitmap of failed modules) in device 88 (device error 0x800)
"show logging onboard" will show log similar to the one below for the reloaded module:
Logging time: Tue Jul 15 19:39:28 2008
machine check: process swapper (0), jiffies 0x744af3a4
Free pages in zone[0]:0x4a70, zone[1]:0x0, zone[2]:0x0
Stack: c000dd58 c001eefc c000b2c4 c000ae98 d2060e10 c003d7a4 c00f869c c0045cdc
d196c584 d196d100 c000c31c c000c3e4 c000ae90 c000c910 c000c924 c0008948 c01ca610
c0000394
.....
.....
```

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: None. The chance of a module reload occurring again on the same module is very rare. Therefore, continued use of the module is acceptable.

A software workaround for this issue exists in SAN-OS Release 3.3.(2) and NX-OS Release 4.(1b). Upgrading to one of those releases will help decrease instances of modules reloads.

- CSCin95789

Symptom: When you configure Cisco Traffic Analyzer to capture traffic on one or more interfaces on a Windows platform, the configuration web page might not show that the interface has been selected for traffic capture even though traffic capture on that interface is enabled.

Workaround: Check the logs to clarify that the correct interface has been selected.

- CSCse31881

Symptom: If there are IP over Fibre Channel (IPFC) interfaces configured on an SSM, you might experience issues if you downgrade from SAN-OS Release 3.x to Release 2.x.

Workaround: Before downgrading, remove the IPFC interface on the module and then recreate the IPFC interface after the downgrade is complete.

- CSCse47687

Symptom: If IP ACLs are applied to any IP Storage Gigabit Ethernet port, implicit deny does not take effect.

Workaround: Configure explicit deny on the port.

- CSCsg19148

Symptom: Time zone changes that are executed on an MDS switch do not take effect on the 12-port, 24-port, and 48 port 1-Gbps/2-Gbps/4-Gbps Fibre Channel modules, and on the 4-port 10-Gbps module. This issue occurs in SAN-OS Releases 3.0(1), 3.0(2), 3.0(2a), and 3.0(3).

Time zone changes that are executed on an MDS switch do not take effect on the 16-port or 32-port 1-Gbps/2-Gbps module, on the 4-port or 8-port Gigabit Ethernet IP services module, the MPS-14/2 module, and on the SSM. This issue occurs in SAN-OS Release 3.0(3).

This issue has no effect on functionality. However, debug messages and syslogs from the MDS switching modules have incorrect timestamps if the time zone is configured on an MDS switch.

Workaround: None.

- CSCsg19303

Symptom: Graceful shutdowns of ISLs are not supported for IVR traffic.

Workaround: Increase the FSPF cost on the link before it is shut down, so that traffic will flow through an alternate path.

- CSCsi66310

Symptom: The management port on MDS switches supports one user-configured IPv6 address, but does not support autoconfiguration of an IPv6 address in Cisco SAN-OS Release 3.2(1).

Workaround: None.

- CSCsj24904

Symptom: On a Gigabit Ethernet interface on an MDS MSM-18/4 module, shut the interface before removing its IP address so that configuration changes on the interface can take effect. This applies only to the Gigabit Ethernet ports in slot 1 of the MDS 9222i switch and the MDS 9216i switch.

Workaround: Always shut the interface using the **shutdown** command before removing the IP address and making configuration changes.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsj72666

Symptom: In certain conditions, an MDS switch may not be able to determine the FC4-type of certain targets. This causes the targets to be listed in the hosts section during a Cisco SME tape group or tape device configuration.

Workaround: Issue the **discover scsi-target vsan vsan-id fcid fcid** command to re-discover the FC4-type of the targets. A Cisco SME tape group or tape device configuration will now list the targets correctly.

- CSCsk06186

Symptom: In rare situations, on an MDS 9513 director switch, an upgrade fails when a standby supervisor does not come up to a state that the installer recognizes. As a result, the standby supervisor is reloaded to recover and the system runs the older configuration version.

Workaround: Perform the upgrade again.

- CSCsk35725

Symptom: Fabric Manager takes 2 to 3 minutes to bring up the DMM job creation wizard in a setup with 25 switches, 400 enclosures, and 2400 entries in the name server.

Workaround: None.

- CSCsk35951

Symptom: In a configuration with a PortChannel with FCIP members and write acceleration in use, if IVR NAT is enabled on one end of the PortChannel and not enabled on the other end, then traffic over the FCIP tunnel might fail.

Workaround: Enable IVR NAT on both ends of the PortChannel or disable it on both ends.

- CSCsk49309

Symptom: IPv6 duplicate address detection (DAD) may not always work for the management port.

Workaround: None.

- CSCsk63929

Symptom: If DMM is provisioned on the SSM and you downgrade to a Cisco MDS SAN-OS release that does not support DMM, the configuration persists and the GUI and CLI show DMM as a provisioned application.

Workaround: Manually remove the DMM configuration from the switch before downgrading to a Cisco MDS SAN-OS release that does not support DMM, such as downgrading from SAN-OS Release 3.2(1) to SAN-OS Release 3.1(3). If you forget to remove the configuration before the downgrade, power off the module and purge the configuration on the SSM module by entering the following commands:

```
switch(config)# poweroff module slot
switch# purge module slot running-config
```

- CSCsk87502

Symptom: If an NASB configuration in a VSAN is destroyed while a target discovery is pending, the NASB process fails. Issue the **show nasb vsan x** command on the SSM to view the target discovery in the Pending state.

Workaround: Reload the SSM.

- CSCsk87614

Symptom: When NASB is enabled in a VSAN, all targets that are visible in that VSAN are discovered by NASB. If a new target is added to the VSAN, NASB does not automatically discover the new target.

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: To discover the new target, reload the SSM or disable and re-enable NASB in the VSAN.

- CSCsk93834

Symptom: In rare situations during a storage-based online data migration job, the user might not be able to destroy the job if the following sequence of events occurs:

1. A storage-based data migration job is executing.
2. A port flap occurs on the server and the server HBA port goes down.
3. The storage-based data migration job continues executing until it completes.
4. The user issues the **dmm module *module-id* job *job-id* destroy** command to delete the storage-based data migration job, but the delete fails.

Workaround: Reload the SSM.

- CSCsk95241

Symptom: If you use JDK instead of JRE on Solaris, you might encounter a problem trying to install Device Manager from a web browser. This can happen because the installer heap limit of 256 MB is not sufficient.

Workaround: If you have this problem, save the `jnl` link as file, increase the heap limit to 512 MB, and run **javaws element-manager.jnl** at the shell prompt.

- CSCsl04532

Symptom: In a VSAN in which a large number of FICON devices exist and FICON tape acceleration is enabled, FICON tape acceleration performance degradation occurs. The FICON devices do not have to be tapes or virtual tapes; for example, they can be disks.

Workaround: None.

- CSCsl12130

Symptom: After a disruptive downgrade or upgrade between SAN-OS Release 3.2(2c) and Release 3.2(1a), issuing a no shutdown command on a Cisco SME interface fails. When issuing the install all command to perform the downgrade process, a warning is issued that indicates that the downgrade will be disruptive if Cisco SME is enabled.

Workaround: Disable Cisco SME before proceeding with the downgrade process. If you perform a disruptive downgrade, then issue the **purge module *slot* running-config** command for the MSM-18/4 modules where Cisco SME is configured after the downgrade is complete.

- CSCsl12611

Symptom: Devices attached on a remote McData switch do not show a correct physical connection on the correct port in Fabric Manager. This occurs because the registered devices in the McData nameserver are shifted by 4 from its actual physical port and Fabric Manager looks at this port address from the nameserver to locate the physical port.

Workaround: None.

- CSCsl15511

Symptom: On the MDS 12-port, 24-port, and 48-port 4-Gbps Fibre Channel switching modules, and on the 4-port 10-Gbps Fibre Channel switching module for downgrades from 3.2(2c) to lower versions, if fcdomain persistency is disabled, F ports may not come up after a **shutdown** or **no shutdown** or a link flap.

Workaround: Shut the F port, enable and disable fcdomain persistency for that VSAN, and then bring up the F port.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsl17944

Symptom: During an MDS 9222i switch reload, the connection from the management port (mgmt0) to the Gigabit Ethernet interface goes down. When the connection comes back up, the Gigabit Ethernet interface doesn't go into forwarding mode until 30 seconds later. The Fabric Manager server is not able to communicate to the MDS 9222i switch through SNMP during this 30 second window.

Workaround: If the switch is in the Cisco Ethernet switch family, configure port-fast to resolve the issue. On Ethernet switches from other vendors, apply a similar configuration mode.

- CSCsl31087

Symptom: In DMM, if a server I/O to a LUN fails during data migration, that session is marked as failed. The DMM migration job is then moved to a Failed state when the remaining sessions are complete. Such a failed migration job can be scheduled for a restart. If such a failed migration job is scheduled to start in less than 5 minutes from the time of scheduling, and another server I/O to a session LUN fails in that 5 minute window, the migration job will move from a Scheduled state to a Failed state. An administrator has the option to start the job immediately or schedule it again. This problem does not happen if an administrator schedules the migration job to start more than 5 minutes from the time of scheduling.

Workaround: Schedule the data migration job to start more than 5 minutes from the time of scheduling.

- CSCsl33763

Symptom: In Cisco SME, tape device names can not include special characters (such as hyphens or underscores). This will cause future tape device creations for a tape group to fail.

Workaround: Use only alpha-numeric values for tape device names.

- CSCsl34922

Symptom: Dual-fabric DMM migration jobs can not have one fabric running Release 3.2(1a) and a peer fabric running Release 3.2(2c) due to a signal message change. This may cause unexpected results during a DMM migration job validation, creation, start, and so on.

Workaround: Run both fabrics with the same software image.

- CSCsm54598

Symptom: When you insert a USB memory device into the usb/1 port, it is shown to be in the usb/2 port; and a USB memory device in a usb/2 port is shown to be in the usb/1 port. This is an ordering issue only; USB functionality is not affected.

Workaround: None.

- CSCso63465

Symptom: FCP-CMD (for example, Inquiry) frames targeted to LUN 0x45F0 or LUN 0x50F0 are dropped by an MDS switch when traffic flows (egresses) thru Generation 2 modules. LUN 0x45F0 corresponds to HP-UX's Volume Set Address <VBUS ID: 0xB, Target ID: 0xE, LUN: 0x0>.

Workaround: Do not use LUN 0x45F0 and LUN 0x50F0 when Generation 2 modules are present in the fabric.

- CSCsi56167

Symptom: The response time shown in the output of a **ping ip-address** command may not be accurate if there is an MDS MSM-8/4 in the path.

Workaround: Use the **ips measure-rtt** command to measure the round trip time.

- CSCsk91974

Symptom: When you issue the **show tech-support sme** or the **show klm internal isapi_scsi** command after attaching to a module, you may see this error message: `cat: write error: Bad address`. This issue does not affect the actual tech-support log.

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: None.

- CSCsk73654

Symptom: In certain tape libraries, the tape drives are exported as LUNs. If these target ports are already a part of a Cisco SME configuration and new tape drives are added as LUNs, the new tape drives will not be discovered during a Cisco SME tape group or tape device configuration.

Workaround: Perform a rescan at the host level or a flap of the target port to allow Cisco SME to rediscover these newly added tape drives.

- CSCsk43927

Symptom: The following Fabric Manager client components that use SSH and Telnet do not work well with NAT:

- DMM storage job creation
- Cisco SAN-OS software upgrade
- Zone activation

Workaround: None.

Send documentation comments to mdsfeedback-doc@cisco.com

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents.

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *Cisco MDS 9000 Family Release Notes for Storage Services Interface Images*
- *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images*

Compatibility Information

- *Cisco MDS 9000 SAN-OS Hardware and Software Compatibility Information*
- *Cisco MDS 9000 Family Interoperability Support Matrix*
- *Cisco MDS Storage Services Module Interoperability Support Matrix*
- *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*

Regulatory Compliance and Safety Information

- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*

Hardware Installation

- *Cisco MDS 9124 Multilayer Fabric Switch Quick Start Guide*
- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*

Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Database Schema*
- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*

Command-Line Interface

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*

Send documentation comments to mdsfeedback-doc@cisco.com

- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*
- *Cisco MDS 9000 Family CLI Quick Configuration Guide*
- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*

Troubleshooting and Reference

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9000 Family SMI-S Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*

Installation and Configuration Note

- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*
- *Cisco 10-Gigabit X2 Transceiver Module Installation Note*
- *Cisco MDS 9000 Family CWDM Installation Note*
- *Cisco MDS 9000 Family CWDM Passive Optical System Installation Note*

Send documentation comments to mdsfeedback-doc@cisco.com

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2008 Cisco Systems, Inc. All rights reserved.

Send documentation comments to mdsfeedback-doc@cisco.com