

Send documentation comments to mdsfeedback-doc@cisco.com



Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.3(3)

Release Date: April 2, 2009

Part Number: OL-14116-11L0

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 46.



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/ps5989/prod_release_notes_list.html

[Table 1](#) shows the online change history for this document.

Table 1 Online History Change

Revision	Date	Description
A0	04/02/2009	Created release notes.
B0	04/16/2009	Added “ FICON Supported Releases and Upgrade Paths ”. Revised “ FICON Downgrade Paths ”.
C0	04/24/2009	Added DDTs CSCsz01738 . Added the “ Compatibility of Fabric Manager and Data Mobility Manager ” limitation.
D0	06/23/2009	Added a statement not to use Java 1.6 Update 13 to the “ The Fabric Manager Installation Process Overview ” section.
E0	07/20/2009	Corrected a typo in the nondisruptive upgrade path information in Table 7 .
F0	07/22/2009	Added DDTs CSCsr85709 . Added the “ Limited ISSU Support on the MDS 9222i Switch ” limitation.



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

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

Table 1 Online History Change (continued)

Revision	Date	Description
G0	08/14/2009	Removed DDTS CSCsm17768 because it was Resolved in SAN-OS Release 3.3(1a).
H0	08/28/2009	Added DDTS CSCso19341 . Added a Note to the “ Installing Fabric Manager on Windows ” section on page -14 about the effect of a Group Policy Object (GPO) in Windows on Fabric Manager Server when used with the PostgreSQL database.
I0	10/09/2009	Added DDTS CSCsv66455 .
J0	11/11/2009	Added DDTS CSCtc48338 .
K0	11/18/2009	Added DDTS CSCsu38485 , CSCtb28442 , CSCtb77695 , and CSCtc20849 .
L0	12/02/2009	Removed the limitation that SANTap is not supported in Release 3.3(3) from the “ Limitations and Restrictions ” section.

Contents

This document includes the following sections:

- [Introduction, page 2](#)
- [Components Supported, page 3](#)
- [Software Download Process, page 8](#)
- [Upgrading Your Cisco MDS SAN-OS Software Image, page 11](#)
- [Downgrading Your Cisco MDS SAN-OS Software Image, page 23](#)
- [New Features in Cisco MDS SAN-OS Release 3.3\(3\), page 26](#)
- [Limitations and Restrictions, page 28](#)
- [Caveats, page 31](#)
- [Related Documentation, page 46](#)
- [Obtaining Documentation and Submitting a Service Request, page 47](#)

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.

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

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	M95S2K9-3.3.3	MDS 9500 Supervisor/Fabric-2, SAN-OS software.	MDS 9500 Series only
	M95S1K9-3.3.3	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S2K9-3.3.3	MDS 9222 Supervisor/Fabric-2, SAN-OS software.	MDS 9200 Series only
	M92S1K9-3.3.3	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S2K9-3.3.3	MDS 9100 Supervisor/Fabric-2, SAN-OS software.	MDS 9100 Series only
	M91S1K9-3.3.3	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only
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

[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	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
	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

[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-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
	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	

[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
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-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).	
	DS-X9148	MDS 9000 48-port 4-Gbps Fibre Channel module (SFPs sold separately).	
	DS-X9704	MDS 9000 4-port 10-Gbps Fibre Channel module (SFPs sold separately)	
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	

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
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.	
	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.	
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.	
	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](mailto: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 8](#)
- [Downloading Software, page 8](#)
- [Selecting the Correct Software Image for an MDS 9200 Series Switch, page 9](#)
- [Migrating from Supervisor-1 Modules to Supervisor-2 Modules, page 10](#)
- [Configuring Generation 2 Switching Modules, page 10](#)

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 the Configuring Generation 2 Switching Modules chapter in the [Cisco MDS 9000 Family CLI Configuration Guide](#).

For information on port index availability, refer to the “Port Index Availability” section in the Product Overview chapter of the [Cisco MDS 9500 Series Hardware Installation Guide](#).

For information on Cisco MDS 9000 hardware and software compatibility, refer to the [Cisco MDS 9000 SAN-OS Hardware and Software Compatibility Information](#).

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

- [Upgrading Your Version of Cisco Fabric Manager, page 11](#)
- [General Upgrading Guidelines, page 15](#)
- [FICON Supported Releases and Upgrade Paths, page 18](#)
- [Upgrading with IVR Enabled, page 18](#)
- [Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.3\(3\), 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](#)
- [Upgrading an MDS 9222i Switch, page 23](#)

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.



Note

When upgrading Fabric Manager, refer to the supported upgrade path shown in [Table 6](#). For example, when upgrading from SAN-OS Release 3.1(x) to Release 3.3(3), you will need to upgrade from Release 3.1(x) to Release 3.2(x) and then upgrade to Release 3.3(3).

Table 6 Supported Fabric Manager Upgrade Paths

Current	Upgrade Path
3.0.x	3.1.x
3.1.x (HSQL)	3.2.x (Oracle)
3.1.x (HSQL)	3.2.x PostgreSQL
3.1.x (Oracle)	3.2.x (Oracle)
3.2.x (Oracle)	3.3.x (Oracle)
3.2.x (PostgreSQL)	3.3.x (PostgreSQL)



Note

Fabric Manager Server can not be installed on an Active Directory Server when using PostgreSQL, Fabric Manager servers are domain controllers and can not create local PostgreSQL user accounts.

Send documentation comments to mdsfeedback-doc@cisco.com

Upgrading from Release 3.1(2c) with the PostgreSQL Patch

To upgrade Fabric Manager to Release 3.3(3) from the UBS special version of 3.1.2c with the PostgreSQL patch, do the following:

-
- Step 1** Upgrade Fabric Manager to Release 3.2(1b), pointing to the same PostgreSQL database which was used by Release 3.1.2c.
 - Step 2** When the installation is complete, stop the Fabric Manager server.
 - Step 3** Run **PM.sh s** located in **\$InstallDir/bin** to re-index the **rrd** files in the PostgreSQL database.
 - Step 4** Upgrade Fabric Manager to Release 3.3(3) by running the Release 3.3(3) installer.
 - Step 5** Discover the fabric again.
 - Step 6** Add the fabric back into the PM collection. This starts the PM collection.
-

The Fabric Manager Installation Process Overview

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 and Device Manager have 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) and JRE 1.6 are supported
 - Java Web Start 1.2, 1.0.1, 1.5, 1.6



Note Do not use Java 1.6 Update 13.

- 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)

Send documentation comments to mdsfeedback-doc@cisco.com

- 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. Refer to [Table 6](#) for information on the supported upgrade path.

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*. Refer to [Table 6](#) for information on the supported upgrade path.

4. 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.
5. 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.

6. 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>

Installing Fabric Manager on Solaris

This section describes how to install Fabric Manager on Solaris.

To install Fabric Manager on Solaris, follow these steps:

-
- Step 1** Set Java 1.5 or 1.6 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.

Send documentation comments to mdsfeedback-doc@cisco.com

- Step 3** Copy the Fabric Manager jar file **m9000-fm-3.3.3.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-3.3.3.jar
```
- Step 5** Follow the onscreen instructions provided in the Fabric Manager management software setup wizard.
- 



### 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.

---

## Installing Fabric Manager on Windows

This section describes how to install Fabric Manager on Windows.



### Note

Fabric Manager Server can not be installed on an Active Directory Server when using PostgreSQL, Fabric Manager servers are domain controllers and can not create local PostgreSQL user accounts.

---



### 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.

---

If your server is running Terminal Services in Application mode, or if you are running Citrix Metaframe or any variation thereof, you need to issue the following command on the DOS prompt before installing Fabric Manager Server.

1. Open a command-line prompt: **Start > Run**, then type **cmd** and press **Return**.
2. At the command prompt type: **user /install**.



### Note

Do not close the command line window. This must remain open for the entire duration of the install.

---

The following is an example of the output of this command:

```
C:\Documents and Settings\user.domain>USER /INSTALL
```

```
User session is ready to install applications.
```

3. Follow all steps needed to install Fabric Manager, Fabric Manager Server, and Device Manager. See the instructions later in this section.

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

- When the installation is complete, at the command prompt, type **user /execute** and press **Return**. Then type **exit** and press **Return**.

The following is an example of the output of this command:

```
C:\Documents and Settings\user.domain>USER /execute
User session is ready to execute applications.
```

To install Fabric Manager on Windows, follow these steps:

- 
- Click the **Install Management Software** link.
  - Choose **Management Software > Cisco Fabric Manager**.
  - Click the **Installing Fabric Manager** link.
  - Select the drive for your CD-ROM.
  - Click the **FM Installer** link.
  - Follow the onscreen instructions provided in the Fabric Manager Installer 3.3(3).
- 

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

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

## General Upgrading Guidelines

Use the following guidelines when upgrading to Cisco MDS SAN-OS Release 3.3(3):

- 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 7](#) 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.
  - 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

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

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 the [“FICON Supported Releases and Upgrade Paths” section on page 18](#).

Use [Table 7](#) to determine your nondisruptive upgrade path to Cisco SAN-OS Release 3.3(3). Find the image release number you are currently using in the Current column of the table and use the path recommended.



**Note**

On an MDS 9222i switch, an upgrade from SAN-OS Release 3.2(x), Release 3.3(1a), or Release 3.3(1c) to SAN-OS Release 3.3(3) fails when there is an active FC-Redirect configuration (created by Cisco SME or Cisco DMM applications) on the switch. An active FC-Redirect configuration is defined as:

- FC-Redirect configuration for hosts or target connected locally
- FC-Redirect configuration created by application running on that switch.

If an upgrade is attempted when an active configurations is present, the switch will go into a disruptive upgrade.



**Note**

The software upgrade information in [Table 7](#) applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and SSM intelligent services traffic.

**Table 7 Nondisruptive Upgrade Path to SAN-OS Release 3.3(3)**

| Current        | Nondisruptive Upgrade Path                                         |
|----------------|--------------------------------------------------------------------|
| SAN-OS 3.3(2)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.3(1c) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.3(1a) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.2(3a) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.2(3)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.2(2c) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.2(1a) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.1(4)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.1(3a) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.1(2b) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.1(2a) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.1(2)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.1(1)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |
| SAN-OS 3.0(3a) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3). |

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

**Table 7 Nondisruptive Upgrade Path to SAN-OS Release 3.3(3) (continued)**

| <b>Current</b> | <b>Nondisruptive Upgrade Path</b>                                                                                                                                                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SAN-OS 3.0(3)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3).                                                                                                                                                                                                                                                |
| SAN-OS 3.0(2a) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3).                                                                                                                                                                                                                                                |
| SAN-OS 3.0(2)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3).                                                                                                                                                                                                                                                |
| SAN-OS 3.0(1)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3).                                                                                                                                                                                                                                                |
| SAN-OS 2.1(3)  | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3).                                                                                                                                                                                                                                                |
| SAN-OS 2.1(2e) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3).                                                                                                                                                                                                                                                |
| SAN-OS 2.1(2d) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3).                                                                                                                                                                                                                                                |
| SAN-OS 2.1(2b) | You can nondisruptively upgrade directly to SAN-OS Release 3.3(3).                                                                                                                                                                                                                                                |
| SAN-OS 2.1(2)  | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.3(3). |
| SAN-OS 2.1(1b) | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.3(3). |
| SAN-OS 2.1(1a) | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.3(3). |
| SAN-OS 2.0(x)  | Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.3(3).<br>or<br>Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.3(3). |
| SAN-OS 1.x     | Upgrade to SAN-OS Release 1.3(4a), then to Release 2.1(2b), and then upgrade to Release 3.3(3).                                                                                                                                                                                                                   |

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

## FICON Supported Releases and Upgrade Paths

Cisco MDS SAN-OS Release 3.3(3) does not support FICON.

Table 8 lists the SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON upgrade path information.

**Table 8** 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) |

## 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:

- 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); you must upgrade to Release 2.1(2b) before upgrading to Release 3.3(3). 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 11](#). 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 **fdomain domain id static vsan vsan id** command to configure the static domains.



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

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

- 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 3.3(3).




---

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

---

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

## Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.3(3)

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 3.3(3).

For more information on upgrading SAN-OS software, see the [“Upgrading Your Cisco MDS SAN-OS Software Image” section on page 11](#).

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
```

- 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
```

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

- 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 NX-OS Release Compatibility Matrix for Storage Service Interface Images](#).
  - All SSM applications are disabled. Use the **show ssm provisioning** command to determine what applications are configured. Use the **no ssm enable feature** command to disable these applications.
  - No SSM ports are in auto mode. See the “[Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.3\(3\)](#)” section on page 20.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module slot epld** 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 Data Center 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

## 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.


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

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

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 3.3(3) on a Cisco MDS 9124 Switch, follow these guidelines:

- 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.

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

## 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 7](#), 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 3.3(3)), 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.

## Upgrading an MDS 9222i Switch

If you are running SAN-OS Release 3.3(3) on an MDS 9222i switch and you want to upgrade to an NX-OS 4.x release, you can upgrade to release 4.1(3a) and higher. Do not attempt to upgrade an MDS 9222i switch from SAN-OS 3.3(3) to NX-OS 4.1(1x) (including 4.1(1b) and 4.1(1c)) because the upgrade path is not supported on the MDS 9222i. This restriction does not apply to other platforms.

Before upgrading, issue the **show install all impact upgrade-image** CLI command to determine if your upgrade will be nondisruptive.

Following the upgrade, you may need to enable features with the **feature feature-name** command, such as the **feature iscsi** command. In SAN-OS 3.3(x) release, features are enabled with the *feature-name enable* command, such as the **iscsi enable** command.

## 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](#)
- [FICON Downgrade Paths, page 25](#)
- [Downgrading the SSI Image on Your SSM, page 26](#)
- [Downgrading an MDS 9222i Switch, page 26](#)

## General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.3(3):

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto: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 the [“FICON Downgrade Paths”](#) section on [page 25](#).

Use [Table 9](#) to determine the nondisruptive downgrade path from Cisco SAN-OS Release 3.3(3). 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 3.3(3)**

| To SAN-OS Release | Nondisruptive Downgrade Path                                           |
|-------------------|------------------------------------------------------------------------|
| SAN-OS 3.3(2)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3). |
| SAN-OS 3.3(1c)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3). |
| SAN-OS 3.3(1a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3). |
| SAN-OS 3.2(3a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3). |
| SAN-OS 3.2(3)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3). |

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

**Table 9 Nondisruptive Downgrade Path from SAN-OS Release 3.3(3)**

| To SAN-OS Release | Nondisruptive Downgrade Path                                                                                    |
|-------------------|-----------------------------------------------------------------------------------------------------------------|
| SAN-OS 3.2(2c)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.2(1a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.1(4)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.1(3a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.1(2b)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.1        | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.1(2)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.1(1)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.0(3a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.0(3)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.0(2a)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.0(2)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 3.0(1)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 2.1(3)     | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 2.1(2e)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).                                          |
| SAN-OS 2.1(2d)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| SAN-OS 2.1(2b)    | You can nondisruptively downgrade directly from SAN-OS Release 3.3(3).                                          |
| 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 SAN-OS Release 3.3(3) does not support FICON.

Refer to [Table 8](#) for a list SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON downgrade path information.

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

## 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 3.3(3) 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 NX-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** command to determine if any applications are provisioned on the SSM. Use the **no ssm enable feature** configuration mode command to disable these features.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module slot epld** 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 Data Center Interoperability Support Matrix](#) and the “Managing Modules” chapter in the [Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x](#), for information on downgrading your SSM.

## Downgrading an MDS 9222i Switch

If you are running MDS NX-OS 4.1(1x) on an MDS 9222i switch and you need to downgrade to a SAN-OS 3.3(x) release, you can downgrade to Release 3.3(2), 3.3(1c), or 3.3(1a), but you cannot downgrade to 3.3(3). A nondisruptive downgrade from NX-OS 4.1(1x) to SAN-OS 3.3(3) is not supported on the MDS 9222i switch. This restriction does not apply to other platforms.

Before downgrading, disable all features not supported by the downgrade release. Use the **show incompatibility system downgrade-image** CLI command to determine what features you need to disable.

Following the downgrade, you will need to enable features with the *feature-name* **enable** command, such as the **iscsi enable** command. In NX-OS 4.1(x) releases, features are enabled with the **feature feature-name** command, such as the **feature iscsi** command.

## New Features in Cisco MDS SAN-OS Release 3.3(3)

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, Release 3.x](#), 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 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.

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

**Note**

---

These release notes are specific to this release. For the complete Release 3.x documentation set, see the [“Related Documentation”](#) section.

---

There are no new features in Cisco MDS SAN-OS Release 3.3(3).

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

## Limitations and Restrictions

This section lists the limitations and restrictions for this release.

### 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`.
  - Step 6** Restart Fabric Manager Server.
- 

### 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.

### Upgrading the SAN-OS Software on the MDS 9222i Switch

On an MDS 9222i switch, an upgrade from SAN-OS Release 3.2(x), Release 3.3(1a), or Release 3.3(1c) to SAN-OS Release 3.3(3) fails when there is an active FC-Redirect configuration (created by Cisco SME or Cisco DMM applications) on the switch. An active FC-Redirect configuration is defined as:

- FC-Redirect configuration for hosts or target connected locally
- FC-Redirect configuration created by application running on that switch.

If an upgrade is attempted when an active configurations is present, the switch will go into a disruptive upgrade.

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

## 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 Storage Media Encryption

The following limitations are described for Cisco SME:

- [Cisco SME Configuration Limits, page 29](#)
- [Deleting Cisco SME Interfaces, page 29](#)
- [Emulex Driver Version, page 30](#)

## Cisco SME Configuration Limits

Table 10 lists the Cisco SME configuration limits for this release.

**Table 10** *Cisco SME Limits*

| Configuration                                | Limit |
|----------------------------------------------|-------|
| Number of switches in the fabric             | 10    |
| Number of clusters per switch                | 1     |
| Switches in a cluster                        | 4     |
| Fabrics in a cluster                         | 2     |
| Modules in a switch                          | 11    |
| Cisco MSM-18/4 modules in a cluster          | 32    |
| Initiator-Target-LUNs (ITLs)                 | 1024  |
| LUNs behind a target                         | 32    |
| Host and target ports in a cluster           | 128   |
| Number of hosts per target                   | 128   |
| 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    |

## Deleting Cisco SME Interfaces

A Cisco SME interface can be deleted from the cluster only after the interface is administratively shut-down and all related tasks associated with the interface shut-down are complete.

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

## Emulex Driver Version

In some instances, the Emulex driver version 8.1.10.9 may set the task attribute to HEAD\_OF\_QUEUE instead of SIMPLE\_QUEUE. Certain tape drives do not accept this attribute and may reject these commands. The Emulex driver version 8.1.10.12 does not have this issue.

## Cisco MDS 9222i Module Upgrade

On the MDS 9222i module, an upgrade from SAN-OS Release 3.2(x) to Release 3.3(1c) is not supported if there is a Cisco SME or Cisco DMM configuration in the fabric for hosts and targets attached to the MDS 9222i module.

## SANTap

The SANTap feature allows third party data storage applications, such as long distance replication and continuous backup, to be integrated into the SAN.

## Deleting SANTap Configurations Is Required Before Downgrade

If you are running Cisco MDS NX-OS Release 4.1(1b) in combination with the SSI 4.1(1b) image and you wish to downgrade to Cisco SAN-OS Release 3.3(3) and an SSI 3.2(3\*) image, you must delete all SANTap configurations prior to the downgrade. Downgrading without completely deleting the SANTap configurations is not supported.

## FCIP Interoperability

FCIP interoperability fails between two MDS switches, one running MDS NX-OS Release 4.1(1c) and the other running MDS SAN-OS Release 3.3(3), if the IP ACL configuration for an IPSec crypto map specifies TCP as the protocol, as in the following example:

```
switch(config)# ip access-list acl-name permit tcp local-gige-ip-address local-mask
remote-gige-ipaddress remote-mask
```

FCIP interoperability does not fail if the IP ACL uses IP as the protocol, as in the following example:

```
switch(config)# ip access-list acl-name permit ip local-gige-ip-address local-mask
remote-gige-ipaddress remote-mask
```

## Applying Zone Configurations to VSAN 1

In the setup script, you can configure system default values for the default-zone to be permit or deny, and you can configure default values for the zone distribution method and for the zone mode.

These default settings are applied when a VSAN is created. However, the settings will not take effect on VSAN 1, because it exists prior to running the setup script. Therefore, when you need these settings for VSAN 1, you must explicitly issue the following commands:

- **zone default-zone permit** *vsan 1*
- **zoneset distribute full** *vsan 1*

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

- zone mode enhanced *vsan 1*

## Running Storage Applications on the MSM-18/4

The Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) does not support multiple, concurrent storage applications. Only one application, such as SME or DMM, can run on the MSM-18/4 at a time.

## 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.

## Limited ISSU Support on the MDS 9222i Switch

An in-service software upgrade (ISSU) from SAN-OS Release 3.3(3) to NX-OS Release 4.1(1b) or to NX-OS Release 4.1(1c) is not supported on the MDS 9222i switch. This limitation applies only to the MDS 9222i switch. You can perform an ISSU from SAN-OS Release 3.3(3) to NX-OS Release 4.1(1b) or NX-OS Release 4.1(1c) on other MDS switches.

ISSU upgrades from SAN-OS Release 3.3(3) to NX-OS Release 4.1(3a) and to NX-OS Release 4.13(a) are supported on the MDS 9222i switch.

## Caveats

This section lists the open and resolved caveats for this release. Use [Table 11](#) to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

**Table 11** Open Caveats and Resolved Caveats Reference

| DDTS Number                | Software Release (Open or Resolved) | Software Release (Open or Resolved) |
|----------------------------|-------------------------------------|-------------------------------------|
|                            | 3.3(2)                              | 3.3(3)                              |
| <b>Severity 1</b>          |                                     |                                     |
| <a href="#">CSCsv66455</a> | O                                   | O                                   |
| <b>Severity 2</b>          |                                     |                                     |
| <a href="#">CSCsc17059</a> | O                                   | R                                   |
| <a href="#">CSCsg49151</a> | O                                   | R                                   |
| <a href="#">CSCsi72048</a> | O                                   | R                                   |
| <a href="#">CSCsk49029</a> | O                                   | R                                   |
| <a href="#">CSCsk49634</a> | O                                   | R                                   |
| <a href="#">CSCsk51193</a> | O                                   | R                                   |
| <a href="#">CSCs139215</a> | O                                   | R                                   |

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

**Table 11** Open Caveats and Resolved Caveats Reference (continued)

| <b>DDTS Number</b>         | <b>Software Release (Open or Resolved)</b> | <b>Software Release (Open or Resolved)</b> |
|----------------------------|--------------------------------------------|--------------------------------------------|
|                            | <b>3.3(2)</b>                              | <b>3.3(3)</b>                              |
| <a href="#">CSCs171227</a> | O                                          | O                                          |
| <a href="#">CSCso19341</a> | O                                          | O                                          |
| <a href="#">CSCso28570</a> | O                                          | R                                          |
| <a href="#">CSCso41087</a> | O                                          | R                                          |
| <a href="#">CSCsq29607</a> | O                                          | R                                          |
| <a href="#">CSCsq44360</a> | O                                          | R                                          |
| <a href="#">CSCsr22782</a> | O                                          | R                                          |
| <a href="#">CSCsr89410</a> | O                                          | R                                          |
| <a href="#">CSCsr92585</a> | O                                          | R                                          |
| <a href="#">CSCsu38485</a> | O                                          | O                                          |
| <a href="#">CSCsw95386</a> | O                                          | R                                          |
| <a href="#">CSCtb28442</a> | O                                          | O                                          |
| <a href="#">CSCtb77695</a> | O                                          | O                                          |
| <a href="#">CSCtc20849</a> | O                                          | O                                          |
| <a href="#">CSCtc48338</a> | —                                          | O                                          |
| <b>Severity 3</b>          |                                            |                                            |
| <a href="#">CSCse31881</a> | O                                          | R                                          |
| <a href="#">CSCsg19148</a> | O                                          | R                                          |
| <a href="#">CSCsg19303</a> | O                                          | R                                          |
| <a href="#">CSCsk35725</a> | O                                          | O                                          |
| <a href="#">CSCsk35951</a> | O                                          | R                                          |
| <a href="#">CSCsk63929</a> | O                                          | R                                          |
| <a href="#">CSCsk87502</a> | O                                          | R                                          |
| <a href="#">CSCsk93834</a> | O                                          | R                                          |
| <a href="#">CSCsk95241</a> | O                                          | R                                          |
| <a href="#">CSCsl15511</a> | O                                          | R                                          |
| <a href="#">CSCsl17944</a> | O                                          | R                                          |
| <a href="#">CSCsl31087</a> | O                                          | R                                          |
| <a href="#">CSCsl34922</a> | O                                          | R                                          |
| <a href="#">CSCsl42571</a> | O                                          | R                                          |
| <a href="#">CSCsl65951</a> | O                                          | R                                          |
| <a href="#">CSCsm08837</a> | O                                          | R                                          |
| <a href="#">CSCsm54071</a> | O                                          | R                                          |
| <a href="#">CSCsm94323</a> | O                                          | R                                          |

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

**Table 11** Open Caveats and Resolved Caveats Reference (continued)

| DDTS Number                | Software Release (Open or Resolved) | Software Release (Open or Resolved) |
|----------------------------|-------------------------------------|-------------------------------------|
|                            | <b>3.3(2)</b>                       | <b>3.3(3)</b>                       |
| <a href="#">CSCso05448</a> | O                                   | R                                   |
| <a href="#">CSCso49196</a> | O                                   | O                                   |
| <a href="#">CSCso55622</a> | O                                   | R                                   |
| <a href="#">CSCso63465</a> | O                                   | R                                   |
| <a href="#">CSCsq20408</a> | O                                   | O                                   |
| <a href="#">CSCsq54455</a> | O                                   | R                                   |
| <a href="#">CSCsq57352</a> | O                                   | R                                   |
| <a href="#">CSCsq66823</a> | O                                   | R                                   |
| <a href="#">CSCsr85709</a> | O                                   | O                                   |
| <a href="#">CSCsr90831</a> | O                                   | R                                   |
| <a href="#">CSCsw78035</a> | O                                   | R                                   |
| <a href="#">CSCsy16228</a> | O                                   | R                                   |
| <a href="#">CSCsz01738</a> | O                                   | O                                   |
| <b>Severity 4</b>          |                                     |                                     |
| <a href="#">CSCsk91974</a> | O                                   | R                                   |
| <b>Severity 5</b>          |                                     |                                     |
| <a href="#">CSCsk73654</a> | O                                   | R                                   |
| <a href="#">CSCso50663</a> | O                                   | R                                   |
| <b>Severity 6</b>          |                                     |                                     |
| <a href="#">CSCsk43927</a> | O                                   | O                                   |
| <a href="#">CSCsm13002</a> | O                                   | R                                   |

## Resolved Caveats

- [CSCsc17059](#)

**Symptom:** In rare circumstances, after upgrading the SAN-OS, a Generation 1 module may be rebooted as it stops responding to the keep alive messages from the Supervisor module.

**Workaround:** This issue is resolved.

- [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:** This issue is resolved.

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

- 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:** This issue is resolved.
- 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:** This issue is resolved.
- CSCsk49634
 

**Symptom:** In rare cases, an FCIP link might flap on a network with high latency and a consistently high loss rate.

**Workaround:** This issue is resolved.
- 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:** This issues is resolved.
- CSCsI39215
 

**Symptom:** The CIM server stops. This occurs after creating a subscription using the same filter and handler.

**Workaround:** This issue is resolved.
- CSCso28570
 

**Symptom:** On the MDS 9222i module, an upgrade from SAN-OS Release 3.2(x) to Release 3.3(1a) fails when there is an active FC-Redirect configuration (created by Cisco SME or Cisco DMM applications) on the switch. An active FC-Redirect configuration is defined as:

  - FC-Redirect configuration for hosts or target connected locally
  - FC-Redirect configuration created by application running on that switch.

If an upgrade is attempted when such active configuration is present, the switch will go into a disruptive upgrade.

**Workaround:** This issue is resolved.
- CSCso41087
 

**Symptom:** If FCIP is enabled and the SAN-OS is upgraded, the SNMP service will run into exception and the following syslog message is displayed: `SNMP Operation(165) failed (62) setting error index.`

**Workaround:** This issue is resolved.

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

- CSCsq29607
 

**Symptom:** After logging back into Fabric Manager Client, clicking on the Summary tab causes a disconnect.

**Workaround:** This issue is resolved..
- CSCsq44360
 

**Symptom:** When the startup rising alarm is triggered, the sample value is smaller than the rising threshold. This should not trigger an alarm.

**Workaround:** This issue is resolved.
- CSCsr22782
 

**Symptom:** On Solaris 8, 9, and 10 and RedHat Linux AS4 (kernel version 2.6) the Fabric Manager Release 3.4(1) installer displays a warning message indicating that it is an unsupported platform. This occurs even though these platforms are supported.

**Workaround:** This issue is resolved.
- CSCsr89410
 

**Symptom:** An FCIP link may flap due to a watchdog timeout condition when FCIP Tape Acceleration is running in SAN-OS Release 3.3(1c).

**Workaround:** This issue is resolved.
- CSCsr92585
 

**Symptom:** An FCIP link running with Tape Acceleration may flap when the host is attempting SRR/REC tape error handling.

**Workaround:** This issue is resolved.
- CSCsu38485
 

**Symptom:** When you enter the **install ssi** command, bootvar fails to synchronize between the active and standby supervisor.

**Workaround:** After the **install ssi** command executes, verify that the SSI bootvar on the standby supervisor is set to the new SSI image. Enter the **show boot** command to display the bootvar configuration. If the SSI bootvar is not set to the proper SSI image, then use the **boot ssi <uri>** command to configure the SSI bootvar on the active supervisor again and verify.
- CSCtb28442
 

**Symptom:** End of sequence is not set for STK drives when the host requests more data than what is written to the tape.

**Workaround:** None.
- CSCtb77695
 

**Symptom:** When a tape reaches its capacity, an IBM TS1120 tape drive send a check condition with eom=1 and asc\_ascq = 0. Because asc\_ascq is not set to End of Medium or Partition, SME continues to send traffic as if the end of the tape has not been reached. As a result, the backup fails when it spans across multiple tapes. This issue is specific only to IBM TS1120 tape drives.

**Workaround:** None.
- CSCtc20849
 

**Symptom:** Following a reboot of an MDS 9513 switch running Cisco SAN-OS Release 3.3(2), both supervisor modules generated core files. The **show cores** command and the **show system reset-reason** command displayed the following output:

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

```

switch# show cores
Module-num Process-name PID Core-create-time

8 qos 15671 Sep 21 22:16
7 qos 4370 Sep 21 22:17

switch# show system reset-reason
----- reset reason for Supervisor-module 8 (from Supervisor in slot 8) ---
1) At 517868 usecs after Mon Sep 21 22:12:09 2009
 Reason: Reset triggered due to HA policy of Reset
 Service: Service "qos"
 Version: 3.3(2)

----- reset reason for Supervisor-module 7 (from Supervisor in slot 7) ---
1) At 260648 usecs after Mon Sep 21 22:12:37 2009
 Reason: Reset triggered due to HA policy of Reset
 Service: Service "qos"
 Version: 3.3(2)

```

**Workaround:** To mitigate the risk of a QoS failure, configure static persistent FC IDs so that the local logins do not share the same domain or area. There should be no more than 50 logins with the same area.

In addition, you can enter the **show qos internal mem-stats detail | inc fcid** command and then check the current allocation value of the QOS\_MEM\_qos\_fcid in the output. If this value is close to 70000, then there is a high chance of a QoS failure, followed by a system reboot.

- CSCsw95386

**Symptom:** Certain applications that use SME perform a **move medium** operation to change tapes in a library, without first performing a **load** or **unload** operation. This causes the check condition “SCSI check condition of medium may have changed.” SME does not perform the media identification logic correctly for this check condition, which causes tape labeling to fail

**Workaround:** This issue is resolved.

- 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:** This issue is resolved.

- 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:** This issue is resolved.

- CSCsg19303

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

**Workaround:** This issue is resolved.

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

- 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:** This issue is resolved.
- 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:** This issue is resolved.
- 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:** This issue is resolved.
- 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:** This issue is resolved.
- 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:** This issue is resolved.
- CSCs115511
 

**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:** This issue is resolved.
- CSCs117944
 

**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:** This issue is resolved.

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

- CSCs131087

**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:** This issue is resolved.
- CSCs134922

**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:** This issue is resolved.
- CSCs142571

**Symptom:** SNMP timeouts occur when a AAA user ages out.

By design, a AAA user is aged out every hour on a switch for security reasons. If a large fabric is discovered using a AAA user and a Performance Monitoring (PM) collection is added for such a fabric, a number of SNMP requests (related to the discovery or PM statistics collection) could time out. When a user views the PM statistics charts (in the Performance tab in the web client), the charts are not seen as continuous.

**Workaround:** This issue is resolved.
- CSCs165951

**Symptom:** Using Fabric Manager Release 3.2(2), an error is displayed in the creation wizard. This occurs when an enclosure spans multiple fabrics and not all fabrics are managed and when the Data Migration Wizard is used to create a job with that enclosure as the existing storage (selecting all ports listed in that enclosure).

**Workaround:** This issue is resolved.
- CSCsm08837

**Symptom:** When an IVR-enabled MDS switch with an empty device alias database, attempts to join a fabric which has approximately 7000 device aliases, the device alias merge fails. In this situation, the following occurs:

  - During the merge process between local and remote switches, the remote device alias database is received on the local switch. The local switch validates those device aliases with SAP 110 (which is IVR).
  - Since all 7000 aliases could not be sent in a single MTS message, the aliases are fragmented into 5 messages.
  - While IVR requires approximately 20 seconds to process each fragment, effectively it takes around 100 seconds to process all 5 messages.
  - Because DDAS has a timeout of around 60 seconds, the merge is rejected.
  - The merge process is retried after few minutes and the process repeats. Then finally failed.

**Workaround:** This issue is resolved.

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

- CSCsm54071  
**Symptom:** Data Virtual Targets (DVTs) are lost after a downgrade from Release 3.3(1x) to earlier releases.  
**Workaround:** This issue is resolved.
- CSCsm94323  
**Symptom:** When a PortChannel is created between 2 switches using the PortChannel wizard in Fabric Manager, the map might not immediately update and may not show the ISLs as part of the PortChannel. After a few discovery cycles, if the map is not updated, then the ISLs may be displayed along with the PortChannel in the map.  
**Workaround:** This issue is resolved.
- CSCso05448  
**Symptom:** FCIP links might fail to come up after a module reload following a hardware failure on the module.  
**Workaround:** This issue is resolved.
- CSCso55622  
**Symptom:** In Microsoft Windows 2000, 2003, 2003 R2, and 2008, when installing Fabric Manager, Fabric Manager Server, and Device Manager, a service may not restart and/or may not properly execute the PostgreSQL installer. This may lead to an incorrect conversion of the PostgreSQL database and/or the service may not start. This occurs when running Microsoft Windows 2000, 2003, 2003 R2, or 2008 with Terminal Server running in Application mode.




---

**Note** This applies only to Terminal Server running in Application Mode. This issue does not affect users running a Terminal Server or Remote Desktop session in Remote Administration mode.

---

**Workaround:** This issue is resolved.

- 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) through Generation 2 modules. LUN 0x45F0 corresponds to HPUX Volume Set Address <VBUS ID: 0xB, Target ID: 0xE, LUN: 0x0>.  
**Workaround:** This issue is resolved.
- CSCsq54455  
**Symptom:** On a DS-X9032 module where the SRAM parity error was seen, the SRAM parity error exceptions were logged continuously.  
**Workaround:** This issue is resolved.
- CSCsq57352  
**Symptom:** After upgrading from Fabric Manager Release 3.0(2a) to Fabric Manager Release 3.2(3a), the Fabric Manager client fails to reuse the map layout files produced by Release 3.0(2a). Renaming the map layout files will make them compatible with Fabric Manager Release 3.2(3a).  
**Workaround:** This issue is resolved.

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

- CSCsq66823

Symptom: On an MDS 9222i switch, an upgrade from SAN-OS Release 3.2(x), Release 3.3(1a), or Release 3.3(1c) to SAN-OS Release 3.3(1c) fails when there is an active FC-Redirect configuration (created by SME or DMM applications) on the switch. An active FC-Redirect configuration is defined as:

- FC-Redirect configuration for hosts or targets connected locally
- FC-Redirect configuration created by the application running on that switch.

If an upgrade is attempted when an active configurations is present, the switch will go into a disruptive upgrade.

**Workaround:** This issue is resolved.

- CSCsr90831

In rare instances, the following Generation 2 modules and MDS switches might reload:

- MDS 900012-port 4-Gbps Fibre Channel switching module
- MDS 9000 24-port 4-Gbps Fibre Channel switching module
- MDS 9000 48-port 4-Gbps Fibre Channel switching module
- MDS 9000 4-port 10-Gbps Fibre Channel switching module
- MDS 9124 Multilayer Fabric Switch
- Cisco Fabric Switch for HP c-Class BladeSystem
- Cisco Fabric Switch for IBM BladeCenter

### Director Switches

The output of the **show logging log** command will have events like those shown below on director switches. 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: JXXXXXXXXX)
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: JXXXXXXXXX)
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: JXXXXXXXXX)
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)
```

The output of the **show logging onboard** command will have a log similar to the one shown below for the reloaded module. To identify the issue in the log, look for one of the following signatures:

```
MCSR: 20000000
MCSR: 10000000

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](mailto:mdsfeedback-doc@cisco.com)**

```

.....
MCSR: 20000000 MCAR:
.....
.....

```

### Fabric Switch and Blade Switches

On affected fabric switch and blades switches, the output of the **show system reset-reason** command will show the following:

```

----- reset reason for Supervisor-module 1 (from Supervisor in slot 1)

1) At 867189 usecs after Tue Aug 12 09:06:25 2008
 Reason: Kernel Panic
 Service:
 Version: 3.2(1a)

```

The output of the **show system exception-info** command will have logs like those shown below on the fabric switch and blade switches. To identify the issue in the log, look for one of the following signatures:

```

MCSR: 40000000
MCSR: 20000000
MCSR: 10000000
MCSR: 00000010

Time of exception: Tue Aug 12 09:06:24 2008
(second=1218503184)
CPU register dump:
1218503184:00960000 machine check: process swapper (0), jiffies
0x6df3d484 Free pages in zone[0]:0xa5c1,zone[1]:0x0,zone[2]:0x0
Call Trace:
 [<c0007298>] [<c0018e44>] [<c000464c>] [<c00041f8>] [<e1db5854>]
 [<e1db8a00>]
 [<e1db5c24>] [<e1db5944>] [<e1dcdafc>] [<e1da8704>] [<e1daad58>]
 [<e1dab17c>]
 [<e1dab4d0>] [<e1d55db8>] [<c001eccc>] [<c00224e8>] [<c001eb98>]
 [<c001ea20>]
 [<c001e654>] [<c00058d0>] [<c00041f0>] [<c0005e20>] [<c0005e34>]
 [<c0001aa8>]
 [<c01c9610>] [<c0000394>]
NIP: E1DB5854 XER: 00000000 LR: E1DB5854 SP: C01B3BE0 REGS: c01b3b30
TRAP: 0200
 Tainted: PF
MSR: 00021000 EE: 0 PR: 0 FP: 0 ME: 1 IR/DR: 00
DEAR: 00000000, ESR: 00000005
MCSRR0: C00044A4, MCSRR1: 00021000, MCAR: 00000000
MCSR: 10000000 MCAR: 00000000 MCPSUMR: 00000000
L2ERRDET: 00000000 L2ERRATTR: 00000000 L2ERRADDR: 00000000
L2ERRCTL: 00000000 L2RSVD: 00000000 PORPLLSR: 00464154
DDRERRDET: 00000000 DDRERRATTR: 00000000 DDRERRADDR: 00000000 TASK =
c01b21d0[0] 'swapper' Last syscall: 120 last math 00000000 last
altivec 00000000 last spe 00000000
.....
.....

```

**Workaround:** This issue is resolved.

- CSCsw78035

**Symptom:** When FlexAttach is enabled on the switch, the physical pWWN in the FCNS registration response is not rewritten with the virtual pWWN.

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

**Workaround:** This issue is resolved.

- CSCsy16228

**Symptom:** Standard variables and user-defined variables are not being substituted in scripts, scheduler jobs, and the CLI.

**Workaround:** This issue is resolved.

- CSCso31754

**Symptom:** IVR does not finish a domain capture which stops the export of IVR devices.

**Workaround:** This issue is resolved.

- 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.

**Workaround:** This issue is resolved.

- 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:** This issue is resolved.

- CSCso50663

**Symptom:** The following syslog message is displayed:

```
%SME_CPP-SLOT13-3-LOG_ERR_SME_ITL_CPP_ERR: Module:13 Host-Target IT Nexus
I:0xc1f3202015180006 T:0xc5a0202000010006 vsan:3000 oid:0x117 LunID:0x0000.
```

This message is for debugging purposes and is also displayed during the upgrade of an MSM-18/4 module. An upgrade of the MSM-18/4 module where Cisco SME is enabled, is disruptive; however, this syslog message does not indicate an issue.

**Workaround:** This issue is resolved.

- CSCsm13002

**Symptom:** In rare cases, if a READ command issued by Cisco SME for media identification is dropped or lost, the tape is marked as a clear-text tape. Subsequently, a CHECK\_CONDITION with ILI is returned when a READ is issued by the host. This can cause a backup application to mark the tape as read-only.

**Workaround:** This issue is resolved.

## Open Caveats

- CSCsv66455

**Symptom:** The management port hangs and does not transmit packets. The following syslog message displays: `eth1: tx timeout`.

**Workaround:** Flap the management port or perform a supervisor switchover.

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

- CSCsl71227

**Symptom:** Using Fabric Manager Release 3.2(2), if you have an enclosure with multiple ports and you then use the Data Migration Wizard to create a job with that enclosure as the existing storage but don't select all the storage ports in the enclosure, an error is displayed in the creation wizard.

**Workaround:** Put the ports you plan to use as the existing storage in the migration into a separate enclosure, and use that enclosure in the wizard selection.

- CSCso19341

**Symptom:** Under very rare circumstances, the ports on an MDS 9000 24-port 4-Gbps Fibre Channel module and on an MDS 9000 48-port 4-Gbps Fibre Channel module might fail and the state of the ports might change to hwFailure, or the module might reload when all the ports on the module fail.

If this occurs, the output of the **show logging log** command will be similar to the following:

```
2008 Mar 12 09:36:47 sw-DC3-Core-9509-1 %PORT-5-IF_DOWN_LINK_FAILURE: %$VSAN 2420%$
Interface fc3/2 is down (Link failure)
2008 Mar 12 09:36:48 sw-DC3-Core-9509-1 %MODULE-2-MOD_DIAG_FAIL: Module 3 (serial:
JAB0938014X) reported failure on ports 3/1-3/6 (Fibre Chan
nel) due to Stratosphere common module experienced an error in device 63 (device error
0xc3f00276)
2008 Mar 12 09:36:48 sw-DC3-Core-9509-1 CSCsu31909 %MODULE-2-MOD_SOMEPORTS_FAILED:
Module 3 (serial: JAB0938014X) reported failure on ports 3/1-3/6 (Fib
re Channel) due to Stratosphere common module experienced an error in device 63 (error
0xc3f00276)
```

Or, the output of the **show logging log** command will be similar to the following:

```
%MODULE-2-MOD_DIAG_FAIL: Module 1 (serial: JABxxxxxxxx) reported failure on ports
1/1-1/24 (Fibre Channel) due to Q-Engine experienced an internal hardware error in
device 55 (device error 0xc3700637)
%MODULE-2-MOD_SOMEPORTS_FAILED: Module 1 (serial: JABxxxxxxxx) reported failure on
ports 1/1-1/24 (Fibre Channel) due to Q-Engine experienced an internal hardware error
in device 55 (error 0xc3700637)
```

The output of the **show module internal exceptionlog** command will be similar to the following:

```
***** Exception info for module 1 *****
exception information --- exception instance 1 ---
Module Slot Number: 1
Device Id : 55
Device Name : Tuscany-que
Device Errorcode : 0xc3700637
Device ID : 55 (0x37)
Device Instance : 00 (0x00)
Dev Type (HW/SW) : 06 (0x06)
ErrNum (devInfo) : 55 (0x37)
System Errorcode : 0x40420032 Q-Engine experienced an internal hardware error
Error Type : Minor error
```

**Workaround:** None.

- CSCtc48338

**Symptom:** On any of the MDS 9500 Series Director switches that have removable Supervisor 2 modules, a supervisor may reset when any one of the following commands is executed on the switch, or the same information is collected through Cisco Fabric Manager or Device Manager:

- **show hardware internal mgmt0 stats**
- **show hardware internal eobc stats**
- **show tech**

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

- **show tech details**
- **show tech-support**
- **tac-pac**

In a dual supervisor switch, entering one of these commands will force a supervisor switchover. In single supervisor systems, the switch will reload.

This issue does not affect switches with a nonremovable Supervisor 2 module, such as the MDS 9222i or MDS 9124.

**Workaround:** There are three ways that you can work around this issue:

- Do not enter the **show hardware internal mgmt0 stats** command or the **show hardware internal eobc stats** command.
- Upgrade to one of the following software releases when it becomes available:  
Cisco SAN-OS Release 3.3(4a) or above  
Cisco NX-OS Release 4.2(3) or above
- Before running the **show tech-support** command, the **show tech-support details** command, or the **tacpac** command from the CLI or from Cisco Fabric Manager or Device manager, download a plug-in from the Software Download Center to patch the commands. Load the plug-in on the active and standby supervisor as described in the following steps. The plug-in is not persistent across switchovers and should be loaded any time a switchover occurs.

To download and install the plug-in, follow these steps:

1. Download the plug-in from  
<http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=282764109>
2. Select release 1.0.
3. Make a copy of the downloaded gplug by entering the following command:  
`switch# copy bootflash:m9500-sup2-showtech-FN63288-plugin-1.0.bin bootflash:gplug_copy`
4. Copy the copy of the gplug to the standby supervisor by entering the following command:  
`switch# copy bootflash:gplug_copy bootflash://sup-remote/`
5. Load the gplug on the active supervisor by entering the following command:  
`switch# load bootflash:gplug_copy`
6. Attach to the standby supervisor by entering the following command:  
`switch# attach module <standby-sup-slot>`
7. Load the gplug on the standby supervisor by entering the following command:  
`switch# load bootflash:gplug_copy`

For additional information, see the Field Notice FN - 63288 that is available at these links:

Guest: <http://www.cisco.com/en/US/ts/fn/632/fn63288.html>

Customer: <http://www.cisco.com/en/US/customer/ts/fn/632/fn63288.html>

- 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.

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

- CSCso49196

**Symptom:** During an upgrade from SAN-OS Release 3.2(3a) to Release 3.3(1a), when a switchover occurs to the Supervisor running Release 3.3(1a), Cisco SME traffic flows for hosts that are not connected locally to the switch that is getting upgraded, may get flapped for a very short time. This can also occur during a switchover to a Supervisor running Release 3.3(1a).

**Workaround:** None.
- CSCsq20408

**Symptom:** After creating SANTap Control Virtual Targets (CVTs) or SANTap Data Virtual Targets (DVTs), the running-configuration and the startup-configuration are not synchronized. Output from the show **startup-config** command will be different from the output of the **show running-config** and the startup configuration will not display SANTap configuration information.

**Workaround:** Issue the **copy running-startup** command whenever you create SANTap Control Virtual Targets (CVTs) or SANTap Data Virtual Targets (DVTs) so that the running configuration and the startup configuration are synchronized.
- CSCsr85709

**Symptom:** Under certain conditions, the port manager can take a long time to respond to a port configuration, which can trigger a set-port-configuration failure. If this occurs, then the FCIP tunnel will not come up and will stay in a disabled state.

**Workaround:** Enter a **shut** command, followed by a **no shut** command on the FCIP interface at either end of the FCIP tunnel.
- CSCsz01738

**Symptom:** A host that is behind a NPIV F port cannot see the zoned LUNs if the addition of the F port to the zone and the zone set activation occur after an In Service Software Upgrade (ISSU). This issue applies only to an NPIV F port on MDS 9124 and MDS 9134 fabric switches.

**Workaround:** Following the ISSU, enter the **shut** command followed by the **no shut** command on the NPIV F port, and then activate the zone set.
- 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](mailto:mdsfeedback-doc@cisco.com)**

## Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at:

[http://www.cisco.com/en/US/products/ps5989/products\\_documentation\\_roadmaps\\_list.htm](http://www.cisco.com/en/US/products/ps5989/products_documentation_roadmaps_list.htm)

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website.

## 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 SAN-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *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 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 Multilayer Fabric Switch Quick Start Guide*
- *Cisco MDS 9020 Fabric Switch 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 Fabric Manager Online Help*

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

- *Cisco MDS 9000 Fabric Manager Web Services Online Help*

## **Command-Line Interface**

- *Cisco MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family CLI Quick Configuration Guide*
- *Cisco MDS 9000 Family CLI Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9000 Family Quick Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*

## **Intelligent Storage Networking Services**

- *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*
- *Cisco MDS 9000 Family Storage Media Encryption Configuration Guide*
- *Cisco MDS 9000 Family Secure Erase Configuration Guide - For Cisco MDS 9500 and 9200 Series*

## **Troubleshooting and Reference**

- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family MIB Quick Reference*
- *Cisco MDS 9020 Fabric Switch MIB Quick Reference*
- *Cisco MDS 9000 Family SMI-S Programming Reference*
- *Cisco MDS 9000 Family System Messages Reference*
- *Cisco MDS 9020 Fabric Switch 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*

## **Obtaining Documentation and Submitting a Service Request**

For information on obtaining documentation, submitting a service request, and gathering additional information, 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>

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

---

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

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (0910R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.