

Send documentation comments to mdsfeedback-doc@cisco.com



Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 3.3(2)

Release Date: November 11, 2008

Part Number: OL-14116-10 O0

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 57.



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	11/11/2008	Created release notes.
B0	11/12/2008	Added DDTs CSCsr89410 and CSCsr92585 .
C0	11/14/2008	Added DDTs CSCso72230 . Corrected the DDTs number of CSCsm32705 .
D0	11/18/2008	Removed DDTs CSCsk90998 .
E0	11/24/2008	Added DDTs CSCso69978 .
F0	11/25/2008	Added DDTs CSCso66705 .
G0	02/04/2009	Added “ Deleting SANTap Configurations Is Required Before Downgrade ” to the Limitations and Restrictions section.
H0	02/24/2009	Added DDTs CSCsq47769 .
I0	03/17/2009	Changed the state of DDTs CSCsc17059 to Resolved.



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

Revision	Date	Description
J0	03/25/2009	Added DDTS CSCsw95386 . Added the “ Storage Media Encryption Not Supported ” limitation.
K0	04/10/2009	Removed descriptions of limitations associated with SME because it is not supported in this release.
L0	04/16/2009	Added “ FICON Supported Releases and Upgrade Paths ”. Revised “ FICON Downgrade Paths ”.
M0	04/24/2009	Added DDTS CSCsz01738 . Added the “ Compatibility of Fabric Manager and Data Mobility Manager ” limitation.
N0	06/23/2009	Added a statement not to use Java 1.6 Update 13 to the “ The Fabric Manager Installation Process Overview ” section.
O0	07/08/2009	Updated the “ SANTap Support ” limitation.

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\(2\), page 26](#)
- [Limitations and Restrictions, page 27](#)
- [Caveats, page 29](#)
- [Related Documentation, page 57](#)
- [Obtaining Documentation and Submitting a Service Request, page 58](#)

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	M95S2K9-3.3.2	MDS 9500 Supervisor/Fabric-2, SAN-OS software.	MDS 9500 Series only
	M95S1K9-3.3.2	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S2K9-3.3.2	MDS 9222 Supervisor/Fabric-2, SAN-OS software.	MDS 9200 Series only
	M92S1K9-3.3.2	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S2K9-3.3.2	MDS 9100 Supervisor/Fabric-2, SAN-OS software.	MDS 9100 Series only
	M91S1K9-3.3.2	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).	MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-X9704	MDS 9000 4-port 10-Gbps Fibre Channel module (SFPs sold separately)	
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.		MDS 9500 Series and 9200 Series, except for the MDS 9216 Switch
	DS-SFP-FC4G-MR	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 4 km.		
	DS-SFP-FC4G-LW	4-Gbps/2-Gbps/1-Gbps Fibre Channel—long wavelength SFP for DS-X91xx switching modules only. Supports distances up to 10 km.		
CWDM ²	DS-CWDM-xxxx	Gigabit Ethernet and 1-Gbps/2-Gbps/4-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm.	MDS 9000 Family	
	DS-CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths.		
	DS-CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths.		
	DS-CWDMCHASSIS	Two slot chassis for CWDM add/drop multiplexers.		
Power supplies	DS-CAC-6000W	6000-W AC power supply.	MDS 9513 only	
	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only	
	DS-CDC-2500W	2500-W DC power supply.		
	DS-CAC-3000W	3000-W AC power supply.		
	DS-CAC-4000W-US	4000-W AC power supply for US (cable attached).		
	DS-CAC-4000W-INT	4000-W AC power supply international (cable attached).		
	DS-CAC-1900W	1900-W AC power supply.		MDS 9506 only
	DS-CDC-1900W	1900-W DC power supply.		
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only	
	DS-CAC-300W	300-W ³ AC power supply.	MDS 9100 Series only	
CompactFlash	MEM-MDS-FLD51M	MDS 9500 supervisor CompactFlash disk, 512 MB.	MDS 9500 Series only	
Port analyzer adapter	DS-PAA-2, DS-PAA	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	MDS 9000 Family	
CD-ROM	M90FMK9-CD322=	MDS 9000 Management Software and Documentation CD-ROM, spare.	MDS 9000 Family	

1. SFP = small form-factor pluggable

2. CWDM = coarse wavelength division multiplexing

3. W = Watt

[Send documentation comments to mdsfeedback-doc@cisco.com](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](mailto: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](#)
- [FICON Supported Releases and Upgrade Paths, page 17](#)
- [Upgrading with IVR Enabled, page 18](#)
- [Reconfiguring SSM Ports Before Upgrading to SAN-OS Release 3.3\(2\), 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 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(2), you will need to upgrade from Release 3.1(x) to Release 3.2(x) and then upgrade to Release 3.3(2).

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(2) 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(2) by running the Release 3.3(2) 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 has been tested with the following software:
 - Windows 2000 SP4, 2003 SP2, XP SP2
 - Redhat Linux (2.6 Kernel)
 - Solaris (SPARC) 8 and 10
 - VMWare Server 1.0:
 - Base Operating System: Windows 2000 SP4 / Virtual Operating System: Windows XP SP2
 - Base Operating System: Windows 2000 SP4 / Virtual Operating System: Windows 2000 SP4
 - Java Sun JRE and JDK 1.5(x) and JRE 1.6 are supported



Note Do not use Java 1.6 Update 13.

- Java Web Start 1.2, 1.0.1, 1.5, 1.6
- Firefox 1.5 and 2.0
- Internet Explorer 6.x, and 7.0



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

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

Send documentation comments to mdsfeedback-doc@cisco.com

- 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.
 - Step 3** Copy the Fabric Manager jar file **m9000-fm-3.3.1c.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-3.3.1c.jar
```

Send documentation comments to mdsfeedback-doc@cisco.com

Step 5 Follow the onscreen instructions provided in the Fabric Manager management software setup wizard.

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.

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.
4. 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:

- Step 1** Click the **Install Management Software** link.
 - Step 2** Choose **Management Software > Cisco Fabric Manager**.
 - Step 3** Click the **Installing Fabric Manager** link.
 - Step 4** Select the drive for your CD-ROM.
 - Step 5** Click the **FM Installer** link.
 - Step 6** Follow the onscreen instructions provided in the Fabric Manager Installer 3.3(2).
-

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

- Step 1** Enter the IP address of the switch in the Address field of your browser.

Send documentation comments to mdsfeedback-doc@cisco.com

- Step 2** Click the **Cisco Device Manager** link in the Device Manager installation window.
- Step 3** Click **Next** to begin the installation.
- Step 4** Follow the onscreen instructions to complete the installation of Device Manager.



Note

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

General Upgrading Guidelines

Use the following guidelines when upgrading to Cisco MDS SAN-OS Release 3.3(2):

- 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 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 17.

Use [Table 7](#) to determine your nondisruptive upgrade path to Cisco SAN-OS Release 3.3(2). 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(2) 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:

Send documentation comments to mdsfeedback-doc@cisco.com

- 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(2)

Current	Nondisruptive Upgrade Path
SAN-OS 3.3(1c)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.3(1a)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.2(3a)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.2(3)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.2(2c)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.2(1a)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.1(4)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.1(3a)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.1(2b)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.1(2a)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.1(2)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.1(1)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.0(3a)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.0(3)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.0(2a)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.0(2)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 3.0(1)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 2.1(3)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 2.1(2e)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 2.1(2d)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 2.1(2b)	You can nondisruptively upgrade directly to SAN-OS Release 3.3(2).
SAN-OS 2.1(2)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.3(2).

Send documentation comments to mdsfeedback-doc@cisco.com

Table 7 *Nondisruptive Upgrade Path to SAN-OS Release 3.3(2) (continued)*

Current	Nondisruptive Upgrade Path
SAN-OS 2.1(1b)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.3(2).
SAN-OS 2.1(1a)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.3(2).
SAN-OS 2.0(x)	Upgrade to SAN-OS Release 2.1(2b) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(2d) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(2e) and then upgrade to Release 3.3(2). or Upgrade to SAN-OS Release 2.1(3) and then upgrade to Release 3.3(2).
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(2).

FICON Supported Releases and Upgrade Paths

Cisco MDS SAN-OS Release 3.3(2) 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)

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

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(2). 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 **fcdomain domain id static vsan vsan id** command to configure the static domains.



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

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



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

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

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

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

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

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

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

Send documentation comments to mdsfeedback-doc@cisco.com

- 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(2).



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(2)

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(2).

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

- 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\(2\)](#)” 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

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(2) 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(2)), the binary startup configuration is deleted because it is not compatible with the new image, and the ASCII startup configuration file is applied when the switch comes up with the new upgraded image. When the ASCII startup configuration file is applied, there may be errors. Because of this, we recommend that you follow the nondisruptive upgrade path.

Downgrading Your Cisco MDS SAN-OS Software Image

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

- [General Downgrading Guidelines, page 23](#)
- [FICON Downgrade Paths, page 25](#)
- [Downgrading the SSI Image on Your SSM, page 25](#)

General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS SAN-OS Release 3.3(2):

- 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.

Send documentation comments to mdsfeedback-doc@cisco.com

- **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(2). 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(2)

To SAN-OS Release	Nondisruptive Downgrade Path
SAN-OS 3.3(1c)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.3(1a)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.2(3a)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.2(3)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.2(2c)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.2(1a)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.1(4)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.1(3a)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.1(2b)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.1	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.1(2)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.1(1)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.0(3a)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.0(3)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.0(2a)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.0(2)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 3.0(1)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
SAN-OS 2.1(3)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).

Send documentation comments to mdsfeedback-doc@cisco.com

Table 9 Nondisruptive Downgrade Path from SAN-OS Release 3.3(2)

To SAN-OS Release	Nondisruptive Downgrade Path
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(2).
SAN-OS 2.1(2b)	You can nondisruptively downgrade directly from SAN-OS Release 3.3(2).
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(2) 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.

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(2) 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.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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.

New Features in Cisco MDS SAN-OS Release 3.3(2)

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.

**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(2).

[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(2) 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

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.

Storage Media Encryption Not Supported

MDS SAN-OS Release 3.3(2) does not support the Storage Media Encryption application because of the open caveat [CSCsw95386](#). A fix for this issue is available in SAN-OS Release 3.3(3) and in NX-OS 4.1(3a). Customers who do not plan to upgrade to SAN-OS Release 3.3(3) or NX-OS Release 4.1(3a), but who need an immediate fix for [CSCsw95386](#) should obtain MDS SAN-OS Release 3.3(2E2), which is a special engineering release for customers who are running SAN-OS Release 3.3(2) and using SME.

You can nondisruptively upgrade from SAN-OS Release 3.3(2) to SAN-OS Release 3.3(2E2). Likewise, you can nondisruptively downgrade from SAN-OS Release 3.3(2E2) to SAN-OS Release 3.3(2).

Cisco MDS 9222i Module Upgrade

On the MDS 9222i module, an upgrade from SAN-OS Release 3.2(x) to Release s 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 Support

The SANTap feature allows third-party data storage applications, such as long distance replication and continuous backup, to be integrated into the SAN. Cisco SAN-OS Release 3.3(2) supports SANTap; however, SSI Release 3.3(2) does not support SANTap.

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(2) 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.

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.

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

Caveats

This section lists the open and resolved caveats for this release. Use [Table 10](#) to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

Table 10 *Open Caveats and Resolved Caveats Reference*

DDTS Number	Software Release (Open or Resolved)	Software Release (Open or Resolved)
	3.3(1c)	3.3(2)
Severity 1		
CSCsu80534	O	R
Severity 2		
CSCsc17059	O	R
CSCsg49151	O	O
CSCsi72048	O	O
CSCsk43922	O	O
CSCsk49029	O	O
CSCsk49634	O	O
CSCsk51193	O	O
CSCsl32492	O	O
CSCsl39215	O	O
CSCsl71227	O	O
CSCsm54544	O	O
CSCso06144	O	R
CSCso28570	O	O
CSCso41087	O	O
CSCso69978	O	R
CSCso72230	O	R
CSCso85603	O	R
CSCsq20470	O	R
CSCsq23079	O	R
CSCsq23098	O	R
CSCsq25023	O	R
CSCsq29607	O	O
CSCSq38724	O	R
CSCsq44360	O	O
CSCsq47769	O	R
CSCsq62770	O	R
CSCsq64637	O	R

Send documentation comments to mdsfeedback-doc@cisco.com

Table 10 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	Software Release (Open or Resolved)
	3.3(1c)	3.3(2)
CSCsq69543	O	R
CSCso72230	O	R
CSCsq78868	O	O
CSCsq80132	O	R
CSCsr22782	—	O
CSCsr11269	O	R
CSCsr59106	O	R
CSCsr62565	O	R
CSCsr70045	O	R
CSCsr71466	O	R
CSCsr79043	O	R
CSCsr89410	O	O
CSCsr92585	O	O
CSCsu03045	O	R
CSCsu31909	O	R
CSCsu44137	O	R
CSCsu48426	O	R
CSCsu68490	O	R
CSCsu90955	O	R
CSCsw95386	—	O
Severity 3		
CSCin95789	O	O
CSCsc67248	O	R
CSCse31881	O	O
CSCse47687	O	O
CSCsg19148	O	O
CSCsg19303	O	O
CSCsi66310	O	O
CSCsj24904	O	O
CSCsj72666	O	O
CSCsj75702	O	R
CSCsk06186	O	O
CSCsk35725	O	O
CSCsk35951	O	O

Send documentation comments to mdsfeedback-doc@cisco.com

Table 10 *Open Caveats and Resolved Caveats Reference (continued)*

DDTS Number	Software Release (Open or Resolved)	Software Release (Open or Resolved)
	3.3(1c)	3.3(2)
CSCsk49309	O	O
CSCsk63929	O	O
CSCsk87502	O	O
CSCsk87614	O	O
CSCsk93834	O	O
CSCsk95241	O	O
CSCs112130	O	O
CSCs115511	O	O
CSCs117944	O	O
CSCs120626	O	R
CSCs131087	O	O
CSCs134922	O	O
CSCs142571	O	O
CSCs165951	O	O
CSCsm08837	O	O
CSCsm39302	O	R
CSCsm47252	O	O
CSCsm54071	O	O
CSCsm63010	O	O
CSCsm68314	O	O
CSCsm90294	O	R
CSCsm94323	O	O
CSCso02848	O	O
CSCso05448	O	O
CSCso49196	O	O
CSCso55622	O	O
CSCso63465	O	O
CSCso65297	O	R
CSCso66705	O	R
CSCso83944	O	R
CSCso87408	O	R
CSCsq15255	O	R
CSCsq17480	O	R
CSCsq17989	O	R

Send documentation comments to mdsfeedback-doc@cisco.com

Table 10 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	Software Release (Open or Resolved)
	3.3(1c)	3.3(2)
CSCsq20408	—	O
CSCsq25859	O	R
CSCsq27248	O	R
CSCsq40292	O	R
CSCsq54455	O	O
CSCsq57352	O	O
CSCsq66823	O	O
CSCsr08325	O	R
CSCsr15094	O	R
CSCsr18556	O	R
CSCsr28197	O	R
CSCsr28302	O	R
CSCsr40527	O	R
CSCsr49173	O	R
CSCsr49954	O	R
CSCsr53531	O	R
CSCsr94621	O	R
CSCsr98144	O	R
CSCsu06940	O	R
CSCsu31223	O	R
CSCsu37199	O	R
CSCsu37854	—	R
CSCsu42003	—	R
CSCsu56780	O	R
CSCsu90793	O	R
CSCsv24238	O	R
CSCsv32082	—	R
CSCsv43094	O	R
CSCsz01738	—	O
Severity 4		
CSCsi56167	O	O
CSCsk91974	O	O
CSCsk73654	O	R
CSCsr02430	O	R

Send documentation comments to mdsfeedback-doc@cisco.com

Table 10 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	Software Release (Open or Resolved)
	3.3(1c)	3.3(2)
CSCsq94831	O	R
CSCsu27719	O	R
CSCsu26064	O	R
Severity 5		
CSCsk73654	O	O
CSCso50663	O	O
Severity 6		
CSCsk43927	O	O
CSCsm13002	O	O
CSCsm15874	O	O
CSCsm17768	O	O
CSCsm18303	O	O
CSCsm32705	O	R
CSCso31469	O	R
CSCsr42622	O	R
CSCsu27719	O	R

Resolved Caveats

- [CSCsu80534](#)

Symptom: An MDS 9124 switch, MDS 9134 switch, MDS 9222i switch, Cisco Fabric Switch for IBM BladeCenter, or Cisco Fabric Switch for HP c-Class BladeSystem, may reboot with reason Unknown or Watchdog Timeout when the switch has been up for 497 days. The following messages may be displayed:

```
switch# show system reset-reason
--- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) No time
Reason: Unknown
Service:
Version: 3.1(2)
or
switch# show system reset-reason
----- reset reason for Supervisor-module 1 (from Supervisor in slot 1) ---
1) At 203437 usecs after Fri Jul 4 18:32:02 2008
Reason: Watchdog Timeout
Service:
Version: 3.1(2)
```

Entering the **show logging onboard** command will contain a card uptime record with an uptime of 497 days.

Send documentation comments to mdsfeedback-doc@cisco.com

```
Thu Sep 25 19:09:33 2008: Card Uptime Record
-----
Uptime: 42946218, 497 days 1 hour(s) 30 minute(s) 18 second(s)
Reset Reason: Unknown (0)
Card Mode.....: Runtime
```

Workaround: This issue is resolved.

- 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.

- CSCso06144

Symptom: Under certain rare circumstances, where there are excessive packet drops in the fabric for a given I/O, port software failure (or in other words, SME engine reset) may be seen due to a race condition between the host side and target side error handling of the exchange. This issue has been observed in stress test scenarios where there are packet drops in the host side and lot of target check conditions for the same I/O.

Workaround: This issue is resolved.

- CSCso69978

Symptom: Following an upgrade from SAN-OS Release 3.2(1) to any higher SAN-OS or NX-OS release on a switch that is deployed in a fabric that is operating in IVR1 (non-NAT) mode, the Fibre Channel name service (FCNS) database may contain partial entries. In particular, the port type is displayed as a dash (-) in the FCNS database.

Workaround: This issue is resolved.

- CSCso85603

Symptom: CPP SME may crash when the port software failure coincides with the forwarding of a SCSI error response from the target.

Workaround: This issue is resolved.

- CSCsq20470

Symptom: If you have more than 7 SME modules in a switch, Fabric Manager Web Client hangs when the cluster summary page is selected.

Workaround: This issue is resolved.

- CSCsq23079

Symptom: The **snmp-server enable trap** CLI command does not support enabling or disabling of traps from the CISCO-IPSEC-PROVISIONING-MIB.

Workaround: This issue is resolved.

- CSCsq23098

Symptom: The **snmp-server enable trap** CLI command does not support enabling or disabling of traps from the CISCO-IMAGE-UPGRADE-MIB.

Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsq25023

Symptom: In rare instances, when the host-side exchange and the target-side exchange map to the same internal hash index, a port software failure due to a watchdog timeout may occur. This issue occurs with a lot of traffic flows through the same SME engine.

Workaround: This issue is resolved.

- CSCsq38724

Symptom: On an MDS 9000 Family switch, after configuring and enabling the Virtual Routing Redundancy Protocol (VRRP) on a Gigabit Ethernet interface, IPS module fails and errors similar to the following are logged:

```
%ETHPORT-5-IF_DOWN_SOFTWARE_FAILURE: Interface GigabitEthernet1/1 is down (Port software failure)
```

This issue affects only the MDS 9222i switch and the DS-X9304-18K9 MSM-18/4 module. It occurs only if the IP default gateway is configured in the same subnet as the VRRP IP address. In most configurations, the IP default gateway is in the mgmt0 subnet. When the IP default gateway is in the mgmt0 subnet, this issue does not occur.

Workaround: This issue is resolved.

- CSCsq47769

Symptom: Under rare circumstances, the internal CompactFlash on the supervisor module can become unresponsive. When this occurs, it is possible for the Online Health Management System (OHMS) process that is monitoring the CompactFlash to hang. The system manager process will detect heart beat failures in the OHMS and will stop and restart it. A core file is created during the restart process.

A file system driver will detect that the CompactFlash has become unresponsive and will mount the root file system as read only. In addition, the **show system health internal plog** command might fail while trying to access persistent log files from the unresponsive CompactFlash. These files will be shown as vsh process cores in the output of the **show cores** command, which is part of the **show tech-support** command.

The **show logging logfile** command will display the following output:

```
2009 Jan 21 18:08:20 mds1 %SYSMGR-3-HEARTBEAT_FAILURE: Service "SystemHealth" sent
SIGABRT for not setting heartbeat for last 3 periods.
2009 Jan 21 18:08:29 mds1 %KERN-3-SYSTEM_MSG: Aborting journal on device ide1(22,3).
2009 Jan 21 18:08:29 mds1 %KERN-2-SYSTEM_MSG: ext3_abort called.
2009 Jan 21 18:08:29 mds1 %KERN-2-SYSTEM_MSG: EXT3-fs abort (device ide1(22,3)):
ext3_journal_start: Detected aborted journal
2009 Jan 21 18:08:29 mds1 %KERN-2-SYSTEM_MSG: Remounting filesystem read-only
2009 Jan 21 18:08:29 mds1 %SYSMGR-3-SERVICE_CRASHED: Service "SystemHealth" (PID 1433)
hasn't caught signal 6 (core saved).
2009 Jan 21 18:08:29 mds1 %SYSTEMHEALTH-4-OHMS_LC_DAEMON_RESTARTED: System Health
process running on module 5 restarted.
```

The **show cores** command will display the following output:

Module-num	Process-name	PID	Core-create-time
5	SystemHealth	1433	Jan 21 18:08
5	vsh	27794	Jan 26 12:11
5	vsh	27797	Jan 26 12:11

This issue is limited to Generation 1 supervisors modules running SAN-OS releases prior to SAN-OS Release 3.3(2), and affects supervisor modules on the following MDS components:

- MDS 9500 Series Switches

Send documentation comments to mdsfeedback-doc@cisco.com

- MDS 9216 Switch
- MDS 9216A Switch
- MDS 9216i Switch
- MDS 9120 Switch
- MDS 9140 Switch

Workaround: This issue is resolved in SAN-OS Release 3.3(2) and NX-OS Release 4.1(1b).

- CSCsq62770

Symptom: Tape device cannot be deleted because an SME process is stuck in wait for discovery.

Workaround: This issue is resolved.

- CSCsc67248

Symptom: The SSH key information is not consistent between the CLI and the SNMP agent. Starting with Release 3.4.1, Fabric Manager and Device Manager will only manage MDS switches running Release 3.4.1 or later for the SSH feature. SSH1(rsa1) support is removed from the CLI, Fabric Manager, and Device Manager starting with Release 3.4.1 to conform with security practices.

Workaround: This issue is resolved.

- CSCsj75702

Symptom: When a tape drive has been created in SME, adding additional paths to the tape drive from newly added hosts does not work from the Fabric Manager Web Client. This indicates that the tape device discovery wizard cannot be used to add these new paths.

Workaround: This issue is resolved.

- CSCsl20626

Symptom: When trying to see if a Watchdog Timeout has occurred on a DS-X9032-SSM module, you may see the following error which indicates the 3rd partition has not been created on the Modflash: file system.

```
MDS-Switch# attach mod 1
Attaching to module 1 ...
To exit type 'exit', to abort type '$.'
```

```
module-1# show system internal watchdog-timeout
Unable to seek /dev/hdc3, error 22
Or
```

```
module-2# show system internal watchdog-timeout
Unable to read /dev/hdc3, error 61
```

This is known to occur on SAN-OS Release 3.0(2a) with the SSI Release 3.0(2) and on the SAN-OS Release 3.1(3a) and SSI Release 3.1(3).

Workaround: This issue is resolved.

- CSCsm39302

Symptom: There is a decrease in the FCIP tunnel throughput when IPsec is configured.

Workaround: This issue is resolved.

- CSCsm90294

Symptom: Certain XSS and XSRF vulnerabilities were found in the Fabric Manager web client.

Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCso65297

Symptom: Though the INTEGER is defined as (-2147483648..2147483647) in SNMPv2-SMI, the range is restricted to a 16Bit value 231 -1 = 2147483647 in the msgId field of the SNMP PDU (as seen in RFC3412).

In the SAN-OS SNMP stack implementation, the agent can potentially return the entire range of INTEGER as the value of msgId before it starts rolling over. This applies to all SNMP notifications generated from MDS switches. This is seen in SAN-OS Release 2.x and 3.x releases.

Workaround: This issue is resolved.

- CSCso66705

Symptom: The FCNS process may fail and dump a core. The process is then gracefully restarted by the system. Because this condition takes a relatively long time to develop, it is unlikely that the FCNS process will fail frequently enough to cause the active supervisor to reboot.

Workaround: This issue is resolved.

- CSCso83944

Symptom: After the first 200 RMON alarms, the SNMP process will start leaking small amounts of memory for each alarm. This eventually causes the SNMP process on the Supervisor module to reach its maximum memory allocation and fail. The Supervisor module will automatically be restarted by SAN-OS. In rare cases, part or all of the SNMP or RMON configuration may be lost. If the SNMP process fails quickly in succession, the active Supervisor module may also reset. If there is a redundant Supervisor module, this will result in a Supervisor switchover.

This occurs only when many RMON alarms are being generated. the SNMPD process may take seconds to hours to fail, depending on the rate of RMON alarms.

This is seen after a SAN-OS upgrade or after RMON alarms have been configured.

Workaround: This issue is resolved.

- CSCso87408

Symptom: A scheduled web report fails to generate when the fabric is deleted from Fabric Manager. The log records Fabric not found fabricID=xxx.

Workaround: This issue is resolved.

- CSCsq15255

Symptom: The output of the **show role session status** command might not have the correct time for the last roles in the CFS session.

Workaround: This issue is resolved.

- CSCsq17480

Symptom: A Supervisor 2 module running on an MDS 9500 switch will reload with Watchdog Timeout reason listed as:

```
`show system reset-reason`
----- reset reason for Supervisor-module 7 (from Supervisor in slot 7)
-----
1) At 363570 usecs after Tue May 6 01:21:22 2008
   Reason: Watchdog Timeout
   Service:
   Version: 3.2(2c)
2) At 347955 usecs after Tue May 6 01:18:48 2008
   Reason: Watchdog Timeout
   Service:
   Version: 3.2(2c)
3) At 110808 usecs after Tue May 6 01:16:13 2008
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
Reason: Watchdog Timeout
Service:
Version: 3.2(2c)
4) At 756666 usecs after Tue May 6 01:13:39 2008
Reason: Watchdog Timeout
Service:
Version: 3.2(2c)
```

Workaround: This issue is resolved.

- CSCsq17989

Symptom: During an upgrade for Release 3.1(3a) to Release 3.2(3a), the standby Supervisor modules is reset due to a global synchronization failure. The following message will be displayed:

```
2008 Apr 30 23:21:39 EX0-ECA-01A %SYSMGR-2-GSYNC_ABORT: Global sync aborted by signal.
2008 Apr 30 23:21:40 EX0-ECA-01A %PLATFORM-5-MOD_REMOVE: Module 5 removed (Serial
number JAB091802TC)
```

If you issue the **show system reset reason** command, an incorrect reason for the reset is shown.

Workaround: This issue is resolved.

- CSCsq25859

Symptom: A DS-X9124 module (module 1 in this case) experienced a D-cache parity error and reloaded by itself. Examples of the log messages are seen below:

```
2008 May 6 09:28:09 SWITCH %MODULE-4-MOD_WARNING: Module 8 (serial: JABxxxxxxxx)
reported warnings on ports 8/1-8/3 (Unknown) due to BE2 Arbiter experienced an error
in device 65 (device error 0xc4102613)
```

```
2008 May 6 09:28:09 SWITCH %MODULE-4-MOD_WARNING: Module 7 (serial: JABxxxxxxxx)
reported warnings on ports 7/1-7/3 (Unknown) due to BE2 Arbiter experienced an error
in device 65 (device error 0xc4102613)
```

```
2008 May 6 09:28:14 SWITCH %XBAR-5-XBAR_STATUS_REPORT: Module 1 reported status for
component 88 code 0x40240015.
```

```
2008 May 6 09:28:14 SWITCH %MODULE-2-MOD_DIAG_FAIL: Module 1 (serial: JABxxxxxxxx)
reported failure on ports 1/1-1/24 (Fibre Channel) due to Fatal runtime Arb error.
(DevErr is bitmap of failed modules) in device 88 (device error 0x1)
```

This caused several other DS-X9124 modules (slots 2-6 in this case) to reset. Examples of log messages are seen below:

```
2008 May 6 09:28:31 SWITCH %MODULE-5-MOD_REINIT: Re-initializing module 5 (serial:
JABxxxxxxxx)
```

```
2008 May 6 09:28:31 SWITCH %MODULE-5-MOD_REINIT: Re-initializing module 6 (serial:
JABxxxxxxxx)
```

```
2008 May 6 09:28:31 SWITCH %MODULE-5-MOD_REINIT: Re-initializing module 4 (serial:
JABxxxxxxxx)
```

```
2008 May 6 09:28:31 SWITCH %MODULE-5-MOD_REINIT: Re-initializing module 3 (serial:
JABxxxxxxxx)
```

```
2008 May 6 09:28:31 SWITCH %MODULE-5-MOD_REINIT: Re-initializing module 2 (serial:
JABxxxxxxxx)
```

This issue will change an arbiter timeout value from 5 seconds to 1.5 seconds in order to prevent other modules from resetting when one resets.

Workaround: This issue is resolved.

- CSCsq27248

Symptom: If some database processes are shut down uncleanly (for example, the host crashes or a process is killed) the following message may be seen:

Send documentation comments to mdsfeedback-doc@cisco.com

```
com.cisco.dcbu.lib.rrd.core.RrdException: Bad sample timestamp
1210312407. Last update time was 9221120237041090560, at
least one second step is required
```

This means that an RRD file has been corrupted.

Workaround: This issue is resolved.

- CSCsq40292

Symptom: The Control Virtual Target (CVT) creation fails.

Workaround: This issue is resolved.

- CSCsr08325

Symptom: The Fabric Manager web client shows Fabric Events with the next description:

```
VSAN ... zone activation success, local switch is 00:00:00:00:00:00:00
```

This issue might occur if the enhanced zone mode is configured for a VSAN.

Workaround: This issue is resolved.

- CSCsr15094

Symptom: If the KMC response comes back with a failure after 10 seconds, it might get stuck in a locked state.

Workaround: This issue is resolved.

- CSCsq94831

Symptom: Typing the Nexus 5000 switch IP address in the browser address bar shows a download page which says Cisco Device Manager for MDS 9000 Series

Workaround: This issue is resolved.

- CSCsu27719

Symptom: PostgreSQL does not shutdown unless it can close all the connections it has. Usually it does not shutdown because it has a connection with Fabric Manager Server.

Workaround: This issue is resolved.

- CSCsu26064

Symptom: When running Fabric Manager 3.2(3) and SAN-OS 3.2(3), go to Fabric Manager > Physical Devices Panel > End Devices > Hosts. The panel that displays in the top right showing the Nx ports does not display all fields for 4GB Qlogic modules. It does not show Model, Firmware or Driver for 4GB Qlogic cards. 2GB Qlogic modules for same switch and FM, show Model, Firmware and Driver.

If you look in Device Manager > FC > Name Server > Advanced tab. In the SymbolicNodeName column you can see HPAE311A FW:v4.00.23 DVR:v9.1.3.16 for the card that does not display correctly in Fabric Manager.

On the switch, if you enter **show fcns data detail** command you can see the symbolic-node-name for the missing HBA.

```
-----
VSAN:10 FCID:0x0a0011
-----
port-wwn (vendor) :50:01:10:a0:00:16:d0:f6
[HOSBILLYGIRL]
node-wwn :50:01:10:a0:00:16:d0:f7
class :3
node-ip-addr :0.0.0.0
ipa :ff ff ff ff ff ff ff ff
```

Send documentation comments to mdsfeedback-doc@cisco.com

```
fc4-types:fc4_features :scsi-fcp:init
symbolic-port-name :
symbolic-node-name :HPAE311A FW:v4.00.23 DVR:v9.1.3.16
port-type :N
port-ip-addr :0.0.0.0
fabric-port-wwn :23:03:00:0d:ec:3b:ad:40
hard-addr :0x000000
permanent-port-wwn (vendor) :50:01:10:a0:00:16:d0:f6
```

The SymbolicNodeName in Device Manager does not get populated into Fabric Manager for Model, Firmware, and Driver.

Workaround: This issue is resolved.

- CSCsr18556

Symptom: License records are not removed if a fabric is purged from the database. License information might be incorrect if the same fabric is added back in to Fabric Manager at a later time.

Workaround: This issue is resolved.

- CSCsr28197

Symptom: The error messages for Device-Alias Merge failures need to be more be enhanced to allow customers to pinpoint offending Device Aliases or pWWNs associated with the merge failure.

Workaround: This issue is resolved.

- CSCsr28302

Symptom: DPVM Merge failure messages need to be enhanced to help customers determine why the merge failed.

Workaround: This issue is resolved.

- CSCsu37199

Symptom: Errors on the management port (mgmt0 or eth1) may be seen in the output of the **show logging log** command.

```
%KERN-3-SYSTEM_MSG: eth1: error in ethGetNextRxBuf %KERN-3-SYSTEM_MSG: eth1: stop
internals failed %KERN-3-SYSTEM_MSG: eth1: error in rx %KERN-3-SYSTEM_MSG: eth1: error
in rx %KERN-3-SYSTEM_MSG: eth1: error in rx %KERN-3-SYSTEM_MSG: eth1: error in rx
%KERN-3-SYSTEM_MSG: eth1: error in rx
```

In rare cases this may result in a kernel panic which causes a supervisor switchover.

Workaround:This issue is resolved.

- CSCsu37854

Symptom: The syslog dialog box in Device Manager does not display all logs.

Workaround: This issue is resolved.

- CSCsu42003

Symptom: When an FCIP tunnel is configured with IPsec between an MDS 9222i switch and an MDS 9216i switch, it fails to come up if an ACL with TCP permit is configured. This causes a mismatch and causes the security association (SA) policy creation to fail in IPsec on the supervisor.

Workaound: This issue is resolved.

- CSCsu56780

Symptom: A Solaris iSCSI host generates this error: iscsi: [ID 498442 kern.warning] WARNING: iscsi session(5) protocol error - received unknown itt:0x0 - protocol error.

Workaround:This issue is resolved

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsu90793

Symptom: Software failures occurred on a Gigabit Ethernet port when FCIP compression mode auto was used.

Workaround: This issue is resolved.
- CSCsv24238

Symptom: If you have host to storage connectivity issues, check the following counters to see if you have increasing packet drops throughout the path that these devices traverse. Use the **show hardware internal packet-flow dropped** command and the **show hardware internal errors all** command to check the counters.

Workaround: This issue is resolved.
- CSCsv32082

Symptom:

Workaround: This issue is resolved.
- CSCsv43094

Symptom: Under rare situations, the MDS 9124 switch might reboot. If you enter the **show system exception-info** command, the log might show information similar to the following:

```
Time of exception: Fri Oct 24 07:06:30 2008(second=1224803190)CPU register
dump:1224803190:00958261 machine check: process feature_mgr (1343), jiffies
0x3d7a6760Free pages in zone[0]:0x6ce1,zone[1]:0x0,zone[2]:0x0Call Trace: [<c0007298>]
[<c0018e44>] [<c000464c>] [<c00041f8>] [<c0055998>] [<c000b474>] [<c0003f48>]
[<10005504>] [<100059fc>] [<0fda00e8>] [<00000000>]
.....
.....
```

Workaround: This issue is resolved.
- CSCsq12364

Symptom: You cannot see information about the default access list for the management interface (mgmt0)which is applied by the system to the management interface (mgmt0)in the absence of any user access list.

Workaround:This issue is resolved.
- CSCsr40527

Symptom: An RDL process crashed because of too many fcpings in a loop. This issue might occur on a switch when fcping is running in a script.

Workaround: This issue is resolved.
- CSCsr49173

Symptom: A network management application may occasionally detect 100% CPU utilization when monitoring an MDS switch via SNMP. The **show process cpu** command does not show a high load. An MDS switch periodically adjusts the hardware clock which can cause the CPU load to reach 100% for less than 1 second. An agent, such as nms, rmon alarm or CLI user, examining the CPU load at this instant will see false CPU load alarms.

Workaround: This issue is resolved.
- CSCsr49954

Symptom: The Recoverpoint Appliance with a QLogic HBA sends an 8 byte RFT_ID instead of the standard 32bytes, which causes FC4 features to be incorrectly registered with all features.

Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsr53531

Symptom: In IVR NAT environment, after active mode PortChannel flaps, some member of the PortChannel may not get programmed in the IVR table, so that related IVR traffic will get lost.

Workaround: This issue is resolved.
- CSCsr94621

Symptom: A Fiber Channel over IP (FCIP) trunk can go down if the maximum transmission unit (MTU in the path is less than the MTU of the MDS Gigabit Ethernet interface.

Workaround: This issue is resolved.
- CSCsr98144

Symptom: If a sync-loss is received for a nonexisting fabric, the xbar-manager transitions to a state from which it does not exit.

Workaround: This issue is resolved.
- CSCsu06940

Symptom: An Octeon core occurred.

Workaround: This problem is resolved.
- CSCsu31223

Symptom: A slow memory leak has been found as a part of the view of the interface table MIB with the SME interfaces. This eventually results in the SNMPD process resetting due to lack of memory.

Workaround: This issue is resolved.
- CSCsr02430

Symptom: After issuing the **show boot** command, there are duplicate image names listed in the switch output as shown below:

```
switch# show boot
sup-1
kickstart variable not set
system variable = bootflash:/m9500-sf1ek9-mzg.3.4.1.bin;bootflash:/m9500-sf1ek9-
mzg.3.4.1.bin
sup-2
kickstart variable not set
system variable = bootflash:/m9500-sf1ek9-mzg.3.4.1.bin;bootflash:/m9500-sf1ek9-
mzg.3.4.1.bin
No module boot variable set
switch#
```

This occurs if you issue the boot system command twice with the same image name as shown below:

```
switch(config)# boot system bootflash:m9500-sf1ek9-mzg.3.4.1.bin
switch(config)# boot system bootflash:m9500-sf1ek9-mzg.3.4.1.bin
```

Workaround: This issue is resolved.
- CSCsq64637

Symptom: All device aliases in Fabric Manager disappear when adding new device aliases.

Workaround: This issue is resolved.
- CSCsq69543

Symptom: Fabric Manager does not update Port Channel changes.

Workaround: This issue is resolved.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCso72230

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

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

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

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

Workaround: This issue is resolved.

The software workaround for this issue helps reduce instances of module reloads, but does not completely eliminate the problem. Consequently, module reloads might still occur.

- CSCsq80132

Symptom: Selecting disks as a part of the tape device configuration causes a CPP SME process failure.

Workaround: This issue is resolved.

- CSCsr11269

Symptom: When fctimer CFS distribution is enabled, no commit can be successful, and no change can be made. The error message is as following:

```
dctl-m9509-190-NAC-B1(config)# fctimer E_D_TOV 1050 vsan 1
Warning:The vsan will be temporarily suspended when updating the timer value
This configuration would impact whole fabric.
Do you want to continue? (y/n) y
2008 Jul 1 11:34:39 dctl-m9509-190-NAC-B1 %CFS-2-MTS_REJECT: Verification failed
reject MTS message SAP 15:RR-token 0x64f82
```

Workaround: This issue is resolved.

- CSCsr59106

Send documentation comments to mdsfeedback-doc@cisco.com

Symptom: For two FCIP links on different modules but sharing a common DS3 pipe, the MDS switch could not saturate the DS3 pipe. In another setup with no latency and min/max-bw configured to 15mbps, the MDS FCIP shaper does not obey bandwidth rules and sends at a rate greater than 15mbps, which caused unnecessary drops in the network. This issue affects the MSM-18/4 module and the MDS 9222i switch.

Workaround: This issue is resolved.

- CSCsr62565

Symptom: With the Cimserver enabled, a zone is created and a device-alias member is added to the zone. Device-alias is in enhanced mode. While querying for ni/ei cisco_zonemembersettingdata, the Cimserver fails.

Workaround: This issue is resolved.

- CSCsr70045

Symptom: An FCIP link with an underlying Ethernet interface set to a large MTU (9000 bytes) flaps whenever data frames are sent. Control traffic (such as tape status check commands) are successful and do not cause flaps. This issue only occurs on an MSM-18/4 modules.

Workaround: This issue is resolved.

- CSCsr71466

Symptom: A CFS de-register message is not sent when IVR is disabled.

Workaround: This issue is resolved.

- CSCsr79043

Symptom: The entries for all configurations are not removed from pss when a VSAN is deleted.

Workaround: This issue is resolved.

- CSCsu03045

Symptom: A module gets stuck in the upgrading state if the LCM gets an error.

Workaround: This issue is resolved.

- CSCsu31909

Symptom: A failure in the internal software on the MSM-18/4 module causes an FCIP link in the PortChannel to drop.

Workaround: This issue is resolved.

- CSCsu44137

Symptom: A downgrade from NX-OS 4.1(1b) to SAN-OS 3.3(1c) is not supported on switches when FC-Redirect based applications like DMM and SME are configured in the fabric, if either of the following conditions are satisfied:

- A target for which FC-Redirect is configured is connected locally, and there are Generation 1 modules with ISLs configured in the switch.
- A host, for which FC-redirect is configured, is connected locally on a Generation 1 module.

In such cases, remove the application configuration for such targets and hosts before proceeding with the downgrade.

Workaround: This issue is resolved.

- CSCsu48426

Send documentation comments to mdsfeedback-doc@cisco.com

Symptom: For a data stream that has a lot of variance in the compression ratio across individual tape blocks on the tape, SME restore performance for the HP LTO drives is substantially affected. However, backup performance is not affected.

Workaround: This issue is resolved.

- CSCsu68490

Symptom: A downgrade from NX-OS 4.1(1b) to SAN-OS 3.1(1) is not supported if there are FC-Redirect configurations and any of the following conditions are true:

- FC-Redirect configuration exists for a locally connected target and if there are ISLs configured on a Generation 2 module.
- FC-Redirect Configuration exists for a locally connected host and if the host is connected to a Generation 2 module.

Downgrading in such cases might lead to traffic disruption and/or data corruption.

Workaround: This issue is resolved.

- CSCsu90955

Symptom: In a dual FCIP link configuration with one of the ports is shutdown, the performance of the other still enabled active FCIP link degrades significantly (from ~12 Mb/sec to 1 Mb/sec).

Workaround: This issue is resolved.

- CSCsm32705

Symptom: Disabling Fabric Manager e-mails for Call Home on a port flap event through the server properties is not allowed.

Workaround: This issue is resolved.

- CSCso31469

Symptom: RMON can not be used to monitor objects for a group of ports of the same type.

Workaround: This issue is resolved.

- CSCsr42622

Symptom: The TSM catalog backup fails due to a limitation in SME where all tape blocks are expected to be 16-byte aligned. This issue has also been observed as part of the TSM Export Node process due to the same reason.

Workaround: None

Open Caveats

- CSCsg49151

Symptom: If you bring up more than one link at a time between two VSANs that have overlapping domains and at least one of the switches is SDV enabled, one link will become isolated. The other links will come up, even though the domains are overlapping. In addition, the SDV virtual domains will change, causing traffic disruption on all devices associated with their old value.

Workaround: Bring up multiple links between two switches one at a time. Verify that the first link came up correctly before attempting to bring up the next link. If the first link fails to come up because of a domain ID overlap, resolve the domain conflict and then try again to bring up the links.

Send documentation comments to 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: If both ends of an FCIP link are not on an MPS-14/2 module, do not use mode 1 and auto.

- CSCsk43922

Symptom: A data path processor (DPP) might fail on an MDS switch running SSI Release 3.2(1) on the SSM. The failure occurs after several days of running traffic when a misbehaving target sends unexpected frames well after the response has already been received from the same target.

Workaround: None.

- CSCsk49029

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

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

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

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

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

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

- CSCsk49634

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

Workaround: None.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsk51193

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

Workaround: Set the port mode to F.
- CSCsl32492

Symptom: Certain drivers cache the PRLI service parameters negotiated across the PLOGI/PRLI session establishment. If a library controller that does not support RETRY FCP-2 error recovery procedures is included in a SME configuration, SME may negotiate RETRY in PRLI with the host. Subsequently, if the library controller is removed from SME, the host driver may cache the PRLI parameter and attempt to perform SRR, which gets rejected by the target.

Workaround: When configuring an SME cluster through the web client, exclude the library controller target ports in the target port selection window. For those tape libraries, where the library controller and tape drives are exported as LUNs behind the target port, this is not an issue.
- CSCsl39215

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

Workaround: Reload the switch.
- 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.
- CSCsm54544

Symptom: In some instances, when requests to the control virtual target (CVT) are made, Fabric Manager times out. Regardless of the timeout, the CVT is created in the specified VSAN.

Workaround: To verify this, do either of the following:

 - Refresh the SANTap CVT field. The CVT will appear.
 - Verify the CVT creation on the Supervisor by issuing the **show santap module <#> cvt** CLI command.
- 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: None. On the MDS 9222i module, an upgrade from SAN-OS Release 3.2(x) to Release 3.3(1a) 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.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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: Disable FCIP during the SAN-OS upgrade.
- CSCsq29607
Symptom: After logging back into Fabric Manager Client, clicking on the Summary tab causes a disconnect.
Workaround: Exit from Fabric Manager Client then restart Fabric Manager Client and log in again.
- 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: None.
- CSCsq78868
Symptom: Flow statistics on a Generation 2 module may not be accurate if any of the flows that participate in flow statistics on the module have multiple FSPF paths.
Workaround: For all flows that have flow statistics configured on that module, make sure there is only one available FSPF path. Use port-channel instead of multiple links to achieve more bandwidth.
- 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: Ignore the warning message and click **Continue**.
- 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: Disable FCIP Tape Acceleration.
- CSCsr92585
Symptom: An FCIP link running with Tape Acceleration may flap when the host is attempting SRR/REC tape error handling.
Workaround: None. If link stability is needed, disable FCIP Tape Acceleration.
- 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: None.
- CSCin95789
Symptom: When you configure Cisco Traffic Analyzer to capture traffic on one or more interfaces on a Windows platform, the configuration web page might not show that the interface has been selected for traffic capture even though traffic capture on that interface is enabled.
Workaround: Check the logs to clarify that the correct interface has been selected.

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCse31881

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

Workaround: Before downgrading, remove the IPFC interface on the module and then recreate the IPFC interface after the downgrade is complete.
- CSCse47687

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

Workaround: Configure explicit deny on the port.
- CSCsg19148

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

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

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

Workaround: None.
- CSCsg19303

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

Workaround: Increase the FSPF cost on the link before it is shut down, so that traffic will flow through an alternate path.
- CSCsi66310

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

Workaround: None.
- CSCsj24904

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

Workaround: Always shut the interface using the **shutdown** command before removing the IP address and making configuration changes.
- CSCsj72666

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

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

Send documentation comments to mdsfeedback-doc@cisco.com

- CSCsk06186

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

Workaround: Perform the upgrade again.
- CSCsk35725

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

Workaround: None.
- CSCsk35951

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

Workaround: Enable IVR NAT on both ends of the PortChannel or disable it on both ends.
- CSCsk49309

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

Workaround: None.
- CSCsk63929

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

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

```
switch(config)# poweroff module slot
switch# purge module slot running-config
```
- CSCsk87502

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

Workaround: Reload the SSM.
- CSCsk87614

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

Workaround: To discover the new target, reload the SSM or disable and re-enable NASB in the VSAN.
- CSCsk93834

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

 1. A storage-based data migration job is executing.

Send documentation comments to mdsfeedback-doc@cisco.com

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

Workaround: Reload the SSM.

- CSCsk95241

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

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

- CSCsl12130

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

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

- CSCsl15511

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

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

- CSCsl17944

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

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

- CSCsl31087

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

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

Send documentation comments to mdsfeedback-doc@cisco.com

- 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: Run both fabrics with the same software image.
- 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: There are two workarounds for this issue. One or both of these workarounds can be used to mitigate this issue.

 - Turn on Interpolation by clicking on the Interpolation check box under **Admin->Configure->Collections** in the web client. This will insure that the charts are continuous in the case of any occasional legitimate timeouts.
 - Use a non-AAA user (for example, use a local user on the switch) for a large fabric discovery and for Performance Monitoring. For provisioning and configuration through the Fabric Manager web client, the user can still be authenticated remotely using AAA.
- 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: 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.
- 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: Enable device alias CFS distribution before enabling IVR.

Send documentation comments to mdsfeedback-doc@cisco.com

- **CSCsm47252**

Symptom: DMM jobs move to the Reset state and the following reason is displayed: `Peer connection failure`. In a Cisco DMM dual-fabric topology, the Storage Service Module (SSMs) in the two fabrics communicate with each other over IP by establishing a TCP connection. This connection is routed IP over FC to the local Supervisor and from the Supervisor it is switched over the IP mgmt interface. As a result, if there is a Supervisor switchover, the TCP connection may or may not survive the switchover. In the event that the TCP connection cannot be re-established in time, the DMM jobs in that SMM will move to the Reset state.

Workaround: None.
- **CSCsm54071**

Symptom: Data Virtual Targets (DVTs) are lost after a downgrade from Release 3.3(1x) to earlier releases.

Workaround: None.
- **CSCsm63010**

Symptom: In SAN-OS Release 3.2(3a) or earlier, Cisco DMM did not include Method1 and Method2 DMM jobs. In those releases, stored configurations were treated implicitly as Method1 DMM jobs. Configurations now stored by SAN-OS Release 3.3(1a) but read by Release 3.2(3a) or earlier, are assumed to be Method1 jobs.

Workaround: None.
- **CSCsm68314**

Symptom: For a storage-based DMM job that is in the Scheduled state, if the server HBA port goes offline, then the scheduled DMM job will not start. Scheduled DMM jobs start only when all server HBA ports and storage ports are up.

Workaround: For scheduled DMM jobs, make sure all server HBA ports and storage ports (both existing and new storage) are up.
- **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: Using Fabric Manager, remove the fabric and then re-discover the fabric.
- **CSCso02848**

Symptom: In Cisco DMM, if a Data Migration Job is configured for an Active-Passive array, only the paths on the active controller of the storage are included as part of the job. (Refer to the *Cisco MDS 9000 Family Data Mobility Manager Configuration Guide*). As a result, if a LUN Trespass has occurred due to a controller fail-over, the host I/Os on the new path to the storage are not captured by DMM and they are not applied to the new storage.

Workaround: If a LUN trespass or controller-failover occurs during migration, destroy the job and recreate it to perform the migration again. This will ensure that the old and new storage are synchronized.
- **CSCso05448**

Symptom: FCIP links might fail to come up after a module reload following a hardware failure on the module.

Workaround: Upgrade to Cisco NX-OS Release 4.1(1b) and reload the module where the failure occurred by entering the **reload module** command..

Send documentation comments to mdsfeedback-doc@cisco.com

- **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: Before you install Fabric Manager, Fabric Manager Server, and Device Manager when using Microsoft Terminal Server in Application mode, you must install the application for global use. This is required when a Service is installed and invoked, and when creating a local dbadmin user. To activate this setting, do the following:

1. Before running the installation script from the Fabric Manager Installation CD, 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.

3. Follow all steps needed to install Fabric Manager, Fabric Manager Server, and Device Manager.
4. When the installation is complete, at the command prompt, type **user /execute** and press **Return**. Then type **exit**.

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

- **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.

- **CSCsq54455**

Symptom: On a DS-X9032 module where the SRAM parity error was seen, the SRAM parity error exceptions were logged continuously.

Workaround: None.

Send documentation comments to mdsfeedback-doc@cisco.com

- 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: Exit all Fabric Manager clients and rename the map layout files by replacing space characters with an underscore. The map layout files are found on the computer running the Fabric Manager server. Each Fabric Manager user has their own directory of map files. These map files are found in the following directory: **C:\Program Files\Cisco Systems\MDS 9000\db\<user>*.map**.
- 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.
- 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.

Workaround: Take the targets in FC-Redirect configurations offline.
- 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.
- CSCso31754

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

Workaround: To avoid the API errors that cause this ACL/IVR issue, enter the **show system internal capability** command on the standby Supervisor and look at the last entry under each module. (You can ignore the Supervisor.) If the output states `online` then you can do a switchover or an upgrade.
- CSCsi56167

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

Workaround: Use the **ips measure-rtt** command to measure the round trip time.
- CSCsk91974

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

Send documentation comments to mdsfeedback-doc@cisco.com

Workaround: None.

- CSCsk73654

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

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

- 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: None.

- 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.

- 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: Unmount and remount the tape from the backup application to resolve this issue.

- CSCsm15874

Symptom: In rare cases, when Cisco SME attempts to perform a tape device discovery of the backend tapes, a SCSI command can stall. This may cause Cisco SME to remain in the device discovery phase.

Workaround: Reload the module.

- CSCsm17768

Symptom: There is a observable performance drop for backup and restore when Cisco SME is introduced between a host and tape due to the increased latency.

Workaround: None.

- CSCsm18303

Symptom: In certain cases with the Tape Recycle policy enabled in Cisco SME, a new key is generated when a tape is recycled and the old key is not purged.

Workaround: Manually purge the older version of the key.

Send documentation comments to 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

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

- *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

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, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, 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 Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, 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. (0807R)

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

© 2008 Cisco Systems, Inc. All rights reserved.

Send documentation comments to mdsfeedback-doc@cisco.com