Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 4.1(1c)

Release Date: December 6, 2008

Part Number: OL-17675-04 W0

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the "Related Documentation" section on page 49.

Note Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*: http://www.cisco.com/en/US/products/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	12/06/2008	Created release notes.
B0	03/13/2009	Removed the limitation "Upgrading the SAN-OS Software on the MDS 9222i Switch." Added the limitations "Applying Zone Configurations to VSAN 1" and "Running Storage Applications on the MSM-18/4".
C0	03/16/2009	Added Oracle 11g Enterprise Edition and Oracle 10g Enterprise Edition to the list of software supported by Cisco Fabric Manager and Device Manager, in the "Upgrading Your Version of Cisco Fabric Manager" section.

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

Table 1 Online History Change (continued)

Revision	Date	Description
D0	03/18/2009	Added DDTS CSCsu23984. Removed the "Upgrading the SAN-OS Software on the MDS 9222i Switch" section. Added the "Applying Zone Configurations to VSAN 1" section. Added the "Running Storage Applications on the MSM-18/4" section.
E0	03/26/2009	Added DDTS CSCsw95386. Added the "Storage Media Encryption Not Supported" limitation.
F0	04/10/2009	Removed descriptions of limitations associated with SME because it is not supported in this release.
G0	04/16/2009	Added FICON Supported Releases and Upgrade Paths. Revised FICON Downgrade Paths, page 30.
H0	04/24/2009	Added DDTS CSCsz01738. Added the "Compatibility of Fabric Manager and Data Mobility Manager" limitation.
I0	06/04/2009	Added SAN-OS Release 3.3(3) to the Nondisruptive Software Upgrade Path information in Table 11 and to the Nondisruptive Software Downgrade Path information inTable 14. Added a statement not to use Java 1.6 Update 13 to the "The Fabric Manager Installation Process Overview" section.
J0	08/03/2009	Added DDTS CSCsu33302 and CSCtb00005. Updated Table 10 with upgrade path from 3.3.x to 4.1.x.
K0	08/31/2009	Added a Note to the "Installing Fabric Manager on Windows" section on page -18 about the effect of a Group Policy Object (GPO) in Windows on Fabric Manager Server when used with the PostgreSQL database.
L0	09/21/2009	Added DDTS CSCsy23429.
M0	10/09/2009	Added DDTS CSCsv66455.
N0	11/11/2009	Added DDTS CSCtc48338.
O0	11/18/2009	Added DDTS CSCtb28442, CSCtb77695, and CSCtc20849.
P0	12/10/2009	Added DDTS CSCsz59152.
Q0	12/23/2009	Added DDTS CSCtc04286 and CSCtd16646.
R0	01/26/2010	Added DDTS CSCsz84411.
S0	04/14/2010	Added the "Determining Software Version Compatibility" section.
T0	07/29/2010	Added the "PPRC Not Supported with FCIP Write Acceleration" limitation.

Table 1 Online History Change (continued)

Revision	Date	Description
U0	10/12/2010	Added DDTS CSCsv20465. Added the Cisco MDS 9500 Series Supervisor-2A module to Table 2.
V0	12/17/2010	Corrected the severity and description of CSCsv20465.
W0	03/11/2012	Updated Table 11 and Table 14.

Contents

This document includes the following:

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.

Cisco MDS 9000 NX-OS Software powers the award winning Cisco MDS 9000 Series Multilayer Switches. It is designed to create a strategic SAN platform with superior reliability, performance, scalability, and features. Formerly known as Cisco SAN-OS, Cisco MDS 9000 NX Software is fully interoperable with earlier Cisco SAN-OS versions and enhances hardware platform and module support.

Components Supported

Table 2 lists the NX-OS software part numbers 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	M95S2K9-4.1.1c	MDS 9500 Supervisor/Fabric-2, NX-OS software.	MDS 9500 Series only
	M92S2K9-4.1.1c	MDS 9200 Supervisor/Fabric-2, NX-OS software.	MDS 9222i Switch only
	M92S1K9-4.1.1c	MDS 9216i Supervisor/Fabric-I, NX-OS software.	MDS 9216i Switch only
	M91S2K9-4.1.1c	MDS 9100 Supervisor/Fabric-2, NX-OS software.	MDS 9124 Switch and MDS 9134 Switch
SSI Interface	SSI-M9K9-411A	Storage Services Interface for NX-OS Release 4.1(1c)	MDS 9000 Family
Licenses	M9500SSE184K9	Storage Services Enabler License for one MSM-18/4 module	MDS 9500 Series only
	M9222ISSE1K9	Storage Services Enabler License	MDS 9222i Switch only
	M9200SSE184K9	Storage Services Enabler License for one MSM-18/4 module	MDS 9200 Series only
	M95DMM184K9	Data Mobility Manager License for one MSM-18/4 module	MDS 9500 Series only
	M9222IDMMK9	Data Mobility Manager License for Cisco MDS 9222i	MDS 9222i Switch
	M92DMM184K9	Data Mobility Manager License for one MSM-18/4 module	MDS 9200 Series only
Licenses (continued)	M95DMM184TSK9	Data Mobility Manager for one MSM-18/4 module — Time Limited to 180 days only	MDS 9500 Series only
	M9222IDMMTSK9	Data Mobility Manager — Time Limited to 180 days only	MDS 9222i Switch only
	M92DMM184TSK9	Data Mobility Manager for one MSM-18/4 module — Time Limited to 180 days only	MDS 9200 Series only

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

Component	Part Number	Description	Applicable Product
Chassis	DS-C9513	Cisco MDS 9513 Multilayer Director (13-slot multilayer director with 2 slots for Supervisor-2 modules, with 11 slots available for switching modules — SFPs sold separately)	MDS 9513 Switch
	DS-C9509	Cisco MDS 9509 Multilayer Director (9-slot multilayer director with 2 slots for Supervisor modules, with 7 slots available for switching modules — SFPs sold separately)	MDS 9509 Switch
	DS-C9506	Cisco MDS 9506 Multilayer Director (6-slot multilayer director with 2 slots for Supervisor modules, with 4 slots available for switching modules — SFPs sold separately)	MDS 9506 Switch
	DS-C9222i-K9	Cisco MDS 9222i Multilayer Fabric Switch (3-rack-unit (3RU) semimodular multilayer fabric switch with 18 4-Gbps Fibre Channel ports, 4 Gigabit Ethernet ports, and a modular expansion slot for Cisco MDS 9000 Family Switching and Services modules)	MDS 9222i Switch
	DS-C9216i-K9	Cisco MDS 9216i Multilayer Fabric Switch(3RU semi-modular multilayer fabric switch with 14 2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, and a modular expansion slot for Cisco MDS 9000 Family Switching and Services modules)	MDS 9216i Switch
	DS-C9134-K9	Cisco MDS 9134 34-Port Multilayer Fabric Switch (1RU fixed-configuration multilayer fabric switch with 32 4-Gbps and 2 10-Gbps Fibre Channel ports)	MDS 9134 Switch
	DS-C9124-K9	Cisco MDS 9124 24-Port Multilayer Fabric Switch (1RU fixed-configuration multilayer fabric switch with 24 4-Gbps Fibre Channel ports)	MDS 9124 Switch
Supervisor Modules	DS-X9530-SF2-K9	Cisco MDS 9500 Series Supervisor-2 Module	MDS 9500 Series
	DS-X9530-SF2A-K9	Cisco MDS 9500 Series Supervisor-2A Module	MDS 9500 Series

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

Component	Part Number	Description	Applicable Product
Switching Modules	DS-X9016	Cisco MDS 9000 16-Port Fibre Channel Switching Module with Small Form-Factor Pluggable (SFP) LC (16-port, 2-Gbps Fibre Channel switching module with SFP LC connectors for Cisco MDS 9216i and Cisco MDS 9500 Series)	MDS 9500 Series MDS 9216i Switch
	DS-X9032	Cisco MDS 9000 32-Port 2-Gbps Fibre Channel Switching Module with SFP LC connectors	MDS 9500 Series MDS 9216i Switch
	DS-X9112	Cisco MDS 9000 12-port 4-Gbps Fibre Channel Switching Module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
	DS-X9124	Cisco 24-port 4-Gbps Fibre Channel Switching Module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
	DS-X9148	Cisco MDS 9000 48-port 4-Gbps Fibre Channel Switching Module with SFP LC	MDS 9500 Series MdS 9200 Series
	DS-X9704	Cisco MDS 9000 Family 4-Port 10-Gbps Fibre Channel Switching Module with SFP LC	MDS 9500 Series MdS 9200 Series
	DS-X9224-96K9	Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series
	DS-X9248-96K9	Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series
	DS-X9248-48K9	Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module with SFP and SFP+ LC connectors	MDS 9500 Series MDS 9222i Switch
Services Modules	DS-X9304-18K9	Cisco MDS 9000 18/4-Port Multiprotocol Services Module (MSM)— 18-port, 4-Gbps Fibre Channel plus 4-port Gigabit Ethernet IP services and switching module with SFP LC connectors	MDS 9500 Series MDS 9200 Series
	DS-X9302-14K9	Cisco MDS 9000 14/2-Port Multiprotocol Services Module — 14-port, 2-Gbps Fibre Channel plus 2-port Gigabit Ethernet IP services and switching module with SFP LC connectors	MDS 9500 Series MDs 9216i Switch
	DS-X9032-SSM	Cisco MDS 9000 32-Port Storage Services Module — 32-port, 2-Gbps storage services module with SFP LC connectors	MDS 9500 Series MDs 9200 Series
External crossbar module	DS-13SLT-FAB1	Cisco MDS 9513 Switching Fabric1 Module	MDS 9513 Switch
	DS-13SLT-FAB2	Cisco MDS 9513 Switching Fabric2 Module	MDS 9513 Switch

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

Component	Part Number	Description	Applicable Product
Optics	DS-X2-FC10G-SR	X2 SC optics, 10-Gbps Fibre Channel for short reach	MDS 9500 Series MDS 9200 Series MDS 9134 Switch
	DS-X2-FC10G-LR	X2 SC optics, 10-Gbps Fibre Channel for long reach (10 km)	MDS 9500 Series MDS 9200 Series MDS 9134 Switch
	DS-X2-FC10G-ER	X2 SC optics, 10-Gbps Fibre Channel for extended reach (40 km)	MDS 9500 Series MDS 9200 Series MDS 9134 Switch
	DS-X2-FC10G-CX4	X2 SC optics, 10-Gbps Fibre Channel over copper	MDS 9500 Series MDS 9200 Series MDS 9134 Switch
	DS-X2-E10G-SR	X2 SC optics, 10-Gbps Ethernet for short reach	MDS 9500 Series MDS 9200 Series

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-FC8G-SW	SFP+ optics (LC type) for 2-, 4-, or 8-Gbps Fibre Channel for shortwave mode	MDS DS-X9200 Series switching modules
	DS-SFP-FC8G-LW	SFP+ optics (LC type) for 2-, 4-, or 8-Gbps Fibre Channel for longwave mode; supports distances up to 10 km	MDS DS-X9200 Series switching modules
	DS-SFP-FC4G-SW	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for shortwave mode	MDS 9124, MDS 9134, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FC4G-MR	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for longwave mode; supports distances up to 4 km	MDS 9124, MDS 9134, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FC4G-LW	SFP optics (LC type) for 1-, 2-, or 4-Gbps Fibre Channel for longwave mode; supports distances up to 10 km	MDS 9124, MDS 9134, MDS 9222i, DS-X9100, and DS-X9200 Series switching modules
	DS-SFP-FC-2G-SW	SFP optics (LC type) for 1- or 2-Gbps Fibre Channel for shortwave mode; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-FC-2G-LW	SFP optics (LC type) for 1- or 2-Gbps Fibre Channel for longwave mode for Cisco MDS 9500, MDS 9200, and MDS 9100 Series; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-FCGE-SW	SFP optics (LC type) for 1-Gbps Ethernet and 1- or 2-Gbps Fibre Channel for shortwave mode; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-FCGE-LW	SFP optics (LC type) for 1-Gbps Ethernet and 1- or 2-Gbps Fibre Channel for longwave mode; not supported for use in 4-Gbps-capable ports	MDS 9000 Series
	DS-SFP-GE-T	SFP (RJ-45 connector) for Gigabit Ethernet over copper	MDS 9000 Series
Cisco Coarse Wavelength-Division Multiplexing (CWDM)	DS-CWDM-xxxx	CWDM Gigabit Ethernet and 1- or 2-Gbps Fibre Channel SFP LC type, where product number xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9000 Family
	DS-CWDM4Gxxxx	CWDM 4-Gbps Fibre Channel SFP LC type, where product number xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9000 Family

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

Component	Part Number	Description	Applicable Product
Dense Wavelength-Division Multiplexing (DWDM)	DWDM-X2-xx.xx	DWDM X2 SC optics for 10-Gbps Fibre Channel connectivity to an existing Ethernet DWDM infrastructure, with 15xx.xx nm wavelength, where xx.xx = 60.61, 59.79, 58.98, 58.17, 56.55, 55.75, 54.94, 54.13, 52.52, 51.72, 50.92, 50.12, 48.51, 47.72, 46.92, 46.12, 44.53, 43.73, 42.94, 42.14, 40.56, 39.77, 38.98, 38.19, 36.61, 35.82, 35.04, 34.25, 32.68, 31.90, 31.12, or 30.33	MDS 9500 Series MDS 9200 Series
	DWDM-SFP-xxxx	DWDM Gigabit Ethernet and 1- or 2-Gbps Fibre Channel SFP LC type, where product number xxxx = 3033, 3112, 3190, 3268, 3425, 3504, 3582, 3661, 3819, 3898, 3977, 4056, 4214, 4294, 4373, 4453, 4612, 4692, 4772, 4851, 5012, 5092, 5172, 5252, 5413, 5494, 5575, 5655, 5817, 5898, 5979, or 6061nm	MDS 9000 Family
Add/Drop Multiplexer (ADM)	DS-CWDMOADM4A	4-channel CWDM optical ADM (OADM) module (Cisco CWDM 1470, 1490, 1510, or 1530 NM Add/Drop Module)	MDS 9000 Family
	DS-CWDMOADM4B	4-channel CWDM OADM module (Cisco CWDM 1550, 1570, 1590, or 1610 NM Add/Drop Module)	MDS 9000 Family
	DS-CWDM-MUX8A	ADM for 8 CWDM wavelengths	MDS 9000 Family
CWDM Multiplexer Chassis	DS-CWDMCHASSIS	2-slot chassis for CWDM ADMs	MDS 9000 Family
Power Supplies	DS-CAC-300W	300W AC power supply	MDS 9100 Series
	DS-C24-300AC	300W AC power supply	MDS 9124 Switch
	DS-CAC-845W	845W AC power supply for Cisco MDS 9200 Series	MDS9200 Series
	DS-CAC-3000W	3000W AC power supply for Cisco MDS 9509	MDS 9509 Switch
	DS-CAC-2500W	2500W AC power supply	MDS 9509 Switch
	DS-CDC-2500W	2500W DC power supply	MDS 9509 Switch
	DS-CAC-6000W	6000W AC power supply for Cisco MDS 9513	MDS 9513 Switch
	DS-CAC-1900W	1900W AC power supply for Cisco MDS 9506	MDS 9506 Switch
CompactFlash	MEM-MDS-FLD512M	External 512-MB CompactFlash memory for supervisor module	MDS 9500 Series
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
Smart Card Reader	DS-SCR-K9	Storage Media Encryption (SME) Smart Card Reader	MDS 9000 Family
Smart Card	DS-SC-K9	SME Smart Card	MDS 9000 Family
CD-ROM	M90FM-CD-441	Cisco MDS 9000 Management Software and Documentation CD-ROM for Cisco MDS 9000 NX-OS Software Release 4.1(1b)	MDS 9000 Family

MDS 9000 Chassis and Module Support in Cisco MDS NX-OS 4.x

Table 3 lists the MDS hardware chassis supported by Cisco MDS NX-OS 4.x.

Table 3 Cisco MDS NX-OS 4.x Chassis Support Matrix

Switch	NX-OS 4.x Support
MDS 9513	Yes
MDS 9509	Yes
MDS 9506	Yes
MDS 9222i	Yes
MDS 9216i	Yes
MDS 9216A	No
MDS 9216	No
MDS 9134	Yes
MD S 9124	Yes
MDS 9140	No
MDS 9120	No
Cisco Fabric Switch for HP c-Class BladeSystem and Cisco Fabric Switch for IBM BladeCenter	Yes

Table 4 lists the MDS hardware modules supported by Cisco MDS NX-OS 4.x. For the list of MDS hardware modules supported by Cisco MDS SAN-OS 3.x, see Table 5.

Table 4 Module Support Matrix for Cisco MDS NX-OS 4.x

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
DS-X9530-SF2-K9	MDS 9500 Supervisor-2Module	Yes	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1Module	No	N/A	N/A
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	Yes[1]	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	Yes[1]	No	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	Yes	Yes	No
DS-X9304-18K9	18/4-Port Multiprotocol Services Module (MSM-18/4)	Yes	Yes	Yes
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes

Table 4 Module Support Matrix for Cisco MDS NX-OS 4.x (continued)

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes
DS-X9308-SMIP	8-port 1-, 2-Gbps IP Switching Module	No	No	No
DS-X9304-SMIP	4-port 1-, 2-Gbps IP Switching Module	No	No	No

1. Requires DS-13SLT-FAB2 in the MDS 9513.

Table 5 lists the MDS hardware modules supported by Cisco MDS SAN-OS 3.x.

Table 5 Module Support Matrix for Cisco MDS SAN-OS 3.x

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i	MDS 9216A	MDS 9216
DS-X9530-SF2-K9	MDS 9500 Supervisor-2 Module	Yes	N/A	N/A	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1 Module	Yes	N/A	N/A	N/A	N/A
DS-X9224-96K9	24-port 8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9248-96K9	48-port 8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9248-48K9	4/44-port Host Optimized8-Gbps Fibre Channel Switching Module	No	No	No	No	No
DS-X9304-18K9	18/4-Port Multiprotocol Services Module (MSM-18/4)	Yes	Yes	Yes	Yes	No
DS-X9112	12-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9124	24-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9148	48-port 4-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9704	4-port 10-Gbps Fibre Channel Switching Module	Yes	Yes	Yes	Yes	No
DS-X9302-14K9	14/2-port Multiprotocol Services (MPS-14/2) Module	Yes	No	Yes	Yes	Yes
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032	32-port 1-, 2-Gbps Fibre Channel Switching Module	Yes	No	Yes	Yes	Yes
DS-X9032-SSM	32-port Storage Services Module (SSM)	Yes	Yes	Yes	Yes	Yes

Table 5 Module Support Matrix for Cisco MDS SAN-OS 3.x (continued)

Module	Description	MDS 9500 Series	MDS 9222i	MDS 9216i	MDS 9216A	MDS 9216
DS-X9308-SMIP	8-port 1-, 2-Gbps IP Switching Module	Yes	No	Yes	Yes	Yes
DS-X9304-SMIP	4-port 1-, 2-Gbps IP Switching Module	Yes	Yes	Yes	Yes	Yes

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*.

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 NX-OS software and includes the following topics:

Determining the Software Version

To determine the version of Cisco MDS NX-OS or 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 NX-OS or 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.

Determining Software Version Compatibility

Table 6 lists the software versions that are compatible in a mixed SAN environment, and the minimum software versions that are supported. We recommend that you use the latest software release supported by your vendor for all Cisco MDS 9000 Family products.

Table 6 Software Version Compatibility

NX-OS Release 5.0(x)	Compatible NX-OS 4.x Versions	Compatible SAN-OS 3.x Versions
NX-OS Release 5.0(1a)	Release 4.1(1b), 4.1(1c), 4.1(3), 4.1(3a), 4.2(1a), 4.2(1b), 4.2(3), 4.2(3a), 4.2(5). Release 4.1(1b) is the minimum supported version.	Release 3.3(1c), 3.3(2), 3.3(3), 3.3(4), 3.3(4a), 3.3(5). Release 3.3(1c) is the minimum supported version.

Downloading Software

The Cisco MDS NX-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 NX-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.

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 7.

.

Table 7 Software Images for MDS 9100 Series Switches

Cisco MDS 9100 Series Switch Type	Supervisor Module Type	Naming Convention
9124, 9134, Cisco Fabric Switch for HP c-Class BladeSystem, Cisco Fabric Switch for IBM BladeCenter	Supervisor-2 module	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 8.

Table 8 Software Images for MDS 9200 Series Switches

Cisco MDS 9200 Series Switch Type	Supervisor Module Type	Naming Convention
9222i	Supervisor-2 module	Filename begins with m9200-s2ek9
9216i		Filename begins with m9200-ek9

Note The m9200-ek9 image should be installed only on the MDS 9216i switch. The MDS 9216 switch and the MDS 9216A switch do not support NX-OS 4.x software. See Table 3 for the list of MDS switches that support Cisco MDS NX-OS 4.x software.

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 9.

Table 9 Software Images for Supervisor Type

Cisco MDS 9500 Series Switch Type	Supervisor Module Type	Naming Convention
9513, 9509, and 9506	Supervisor-2 module	Filename begins with m9500-sf2ek9

Use the **show module** command to display the type of supervisor module in the switch. The following is sample output from the **show module** command on a Supervisor 2 module:

```
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
```

Upgrading Your Cisco MDS NX-OS Software Image

This section lists the guidelines recommended for upgrading your Cisco MDS NX-OS software image and includes the following topics:

Note Before you begin the upgrade process, review the list of chassis and modules that NX-OS Release 4.1(1c) supports. See the "MDS 9000 Chassis and Module Support in Cisco MDS NX-OS 4.x" section on page 10.

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 NX-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 10. For example, when upgrading from SAN-OS Release 3.1(x) to NX-OS Release 4.1, you will need to upgrade from Release 3.1(x) to Release 3.2(x) to Release 3.3(x) and then upgrade to NX-OS Release 4.1(1c)

Table 10 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)
3.3.x (Oracle)	4.1.x (Oracle
3.3.x (PostgreSQL)	4.1.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.

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.

Caution Windows 2000 is incompatible with Cisco Fabric Manager Release 4.1(1c). If you are currently running Windows 2000, Cisco strongly recommends that you update your environment before you begin the installation of Fabric Manager. This section lists the supported software that has been tested with Cisco Fabric Manager. See Table 10 for the supported upgrade paths for Cisco Fabric Manager.

1. Verify supported software. Cisco Fabric Manager has been tested with the following software:
   - Windows 2003 SP2, XP SP2, Windows Vista
   - Red Hat Enterprise Linux (AS Release 4)
   - Solaris (SPARC) 8, 9, and 10
   - VMWare ESX 3.5:
   - Virtual Operating System: Windows 2003 SP2
   - 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
- Oracle 11g Enterprise Edition
- Oracle 10g Enterprise Edition
- Oracle Database 10g Express
- PostgreSQL 8.2 (Windows and Linux)
- PostgreSQL 8.1 (Solaris)
- Cisco ACS 3.1 and 4.0
- PIX Firewall
- IP Tables
- SSH v2
- Global Enforce SNMP Privacy Encryption
- HTTPS

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

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

3. Ensure data migration when upgrading Cisco Fabric Manager from releases prior to Cisco NX-OS Releases 4.1(1c).

   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 10 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-4.1.1c.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-4.1.1c.jar
```

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.

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

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

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

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

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

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

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

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

3. Follow all steps needed to install Fabric Manager, Fabric Manager Server, and Device Manager. See the instructions later in this section.
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(1c).

Caution Windows 2000 is incompatible with Fabric Manager Release 4.1(1c). If you install Fabric Manager in a Windows 2000 environment, you are at risk of having an unstable Fabric Manager. Cisco strongly recommends that you exit the installation and update your environment. See "The Fabric Manager Installation Process Overview" section on page 16 for the list of supported software that has been tested with Cisco Fabric Manager. See Table 10 for the supported upgrade paths for Fabric Manager.

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

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

Step 2 Click the **Cisco Device Manager** link in the Device Manager installation window.

Step 3 Click **Next** to begin the installation.

Step 4 Follow the onscreen instructions to complete the installation of Device Manager.

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

General Upgrading Guidelines

Note To upgrade to NX-OS Release 4.1(1c)) from SAN-OS Release 3.2(3a) or earlier, first upgrade to SAN-OS Release 3.3(x) and then upgrade to NX-OS Release 4.1(1c).

Use the following guidelines when upgrading to Cisco MDS NX-OS Release 4.1:

- 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 or MDS 9134 Switch as described in "Upgrading a Cisco MDS 9124 or Cisco MDS 9134 Switch" section on page 27.
- 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 28.
- 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 11 for the nondisruptive upgrade path for all NX-OS and 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 23 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 22.

Note In addition to these guidelines, you may want to review the information in the "Limitations and Restrictions" section prior to a software upgrade to determine if a feature may possibly behave differently following the upgrade.

Use Table 11 to determine your nondisruptive upgrade path to Cisco MDS NX-OS Release 4.1(1c), 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, if SANTap or Invista is provisioned on a Storage Services Module (SSM) in slot2, then an In Service Software Upgrade (ISSU) to NX-OS Release 4.1(1c) is not supported. The upgrade to NX-OS Release 4.1(1c) is supported if you set boot variables, save the configuration, and reload the switch. If the switch is running SAN-OS Release 3.3(1a) or earlier, first upgrade to SAN-OS Release 3.3(1c) and then upgrade to NX-OS Release 4.1(1c).

Note The software upgrade information in Table 11 applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and SSM intelligent services traffic.

Table 11 Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 4.1(1c)

Current Release	Nondisruptive Upgrade Path and Ordered Upgrade Steps
NX-OS:	
Release 4.1(1b)	1. Upgrade to NX-OS Release 4.1(1c).
SAN-OS:	
Release 3.3(1c), 3.3(2), 3.3(3), 3.3(4x), and 3.3(5x).	1. Upgrade to NX-OS Release 4.1(1c).
Release 3.2(1a), all 3.2(x), 3.1(x), and 3.0(x) releases, and release 2.1(3), 2.1(2e), 2.1(2d), and 2.1(2b)	1. Upgrade to SAN-OS Release 3.3(1c). 2. Upgrade to NX-OS Release 4.1(1c).
Release 2.1(2), 2.1(1b), 2.1(1a), and 2.0(x)	1. Upgrade to SAN-OS Release 2.1(2b), 2.1(2d), 2.1(2e), or 2.1(3). 2. Upgrade to SAN-OS Release 3.3(1c). 3. Upgrade to NX-OS Release 4.1(1c).
Release 1.x	1. Upgrade to SAN-OS Release 1.3(4a). 2. Upgrade to SAN-OS Release 2.1(2b). 3. Upgrade to SAN-OS Release 3.3(1c). 4. Upgrade to NX-OS Release 4.1(1c).

FICON Supported Releases and Upgrade Paths

Cisco MDS NX-OS Release 4.1(1c) supports FICON.

Table 12 lists additional SAN-OS and NX-OS releases that also support FICON. Refer to the specific release notes for FICON upgrade path information.

Table 12 FICON Supported Releases

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

Use Table 13 to determine your FICON nondisruptive upgrade path to Cisco MDS NX-OS Release 4.1(1c) Find the image release number you are currently using in the Current Release with FICON Enabled column of the table and follow the recommended path.

Table 13 FICON Nondisruptive Upgrade Path to NX-OS Release 4.1(1c)

Current Release with FICON Enabled	Upgrade Path
SAN-OS 3.3(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.1(1c)
SAN-OS 3.2(2c)	First upgrade to SAN-OS Release 3.3(1c) and then upgrade to NX-OS Release 4.1(1c)
SAN-OS 3.0(3b)	First upgrade to SAN-OS Release 3.3(1c) and then upgrade to NX-OS Release 4.1(1c)
SAN-OS 3.0(2)	First upgrade to SAN-OS Release 3.3(1c) and then upgrade to NX-OS Release 4.1(1c)
SAN-OS 3.0(1) and earlier	First upgrade to SAN-OS Release 3.3(1c) and then upgrade to NX-OS Release 4.1(1c)
SAN-OS 2.0(2b)	Use the **interface shutdown** command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively upgrading from SAN-OS Release 2.0(2b) to SAN-OS Release 3.0(2) or SAN-OS Release 3.0(3b), and then upgrade to Release 3.3(1c). An operationally down state includes `Link failure or not-connected`, `SFP not present`, or `Error Disabled` status in the output of a **show interface** command. When an interface is administratively shut it will then show as `Administratively down`. Interfaces that are currently up or trunking do not need to be shut down.
SAN-OS 1.x	Upgrade to SAN-OS Release 3.0(2). Use the **interface shutdown** command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively upgrading to Release 2.0(2b) and then upgrade to 1.3(4a).

Upgrading with IVR Enabled

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

- 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(1c). 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 15. 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
PortChannel 52 (reason: unknown failure)
2005 Aug 31 21:52:04 switch %FCDOMAIN-2-EPORT_ISOLATED: %$VSAN 2005%$
Isolation of interface PortChannel 51
(reason: domain ID assignment failure)
```

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

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

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

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

Step 7 Follow the normal upgrade guidelines for Release 2.1(2b). If you are adding new switches running Cisco MDS SAN-OS Release 2.1(2b) or later, upgrade all of your existing switches to Cisco SAN-OS Release 2.1(2b) as described in this workaround. Then follow the normal upgrade guidelines for Release 3.3(1c).

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

Reconfiguring SSM Ports Before Upgrading to NX-OS Release 4.1(1c)

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(1c) to NX-OS Release 4.1(1c)

For more information on upgrading SAN-OS software, see the "Upgrading Your Cisco MDS NX-OS Software Image" section on page 15.

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
```

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 NX-OS Release 4.1(1c)" section on page 25.
  - 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

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 or Cisco MDS 9134 Switch

If you are upgrading from Cisco MDS SAN-OS Release 3.1(1) to Cisco NX-OS Release 4.1 on a Cisco MDS 9124 or MDS 9134 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.

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 11, 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 NX-OS Release 4.1), 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 includes the following topics:

Note If you plan to downgrade from NX-OS 4.1(1c) to a SAN-OS 3.x release, read the instructions in the "Downgrading from NX-OS 4.x to SAN-OS 3.x" section on page 31 before you begin.

General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS NX-OS Release 4.1(1c):

- 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* command to determine what you need to disable.
- Use the **show install all impact** *downgrade-image* 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 14 for the nondisruptive downgrade path for all SAN-OS releases.

- **SSM**: Intelligent services traffic on the SSM, such as SANTap, NASB, and FC write acceleration, is disrupted during a downgrade. SSM Fibre Channel traffic is not.
- **Gigabit Ethernet Ports**: Traffic on Gigabit Ethernet ports is disrupted during a downgrade. This includes IPS modules and the Gigabit Ethernet ports on the MPS-14/2 module, the MSM-18/4 module, and the MDS 9222i switch. Those nodes that are members of VSANs traversing an FCIP ISL are impacted, and a fabric reconfiguration occurs. iSCSI initiators connected to the Gigabit Ethernet ports lose connectivity to iSCSI targets while the downgrade is in progress.
- **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 23 for these instructions.
- **FICON**: If you have FICON enabled, the downgrade path is different. See the "FICON Downgrade Paths" section on page 30.

Note A downgrade from NX-OS Release 4.1(1c) to SAN-OS Release 3.3(1x) is not supported on MDS switches, when FC-Redirect based applications, such as Data Mobility Manager or Storage Media Encryption, are configured in the fabric if either of the following conditions are satisfied:

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

If these conditions exist, remove the application configuration for these targets and hosts before proceeding with the downgrade.

Use Table 14 to determine the nondisruptive downgrade path from Cisco NX-OS Release 4.1(1c) 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 14 applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and SSM intelligent services traffic.

Table 14 Nondisruptive Downgrade Path from NX-OS Release 4.1(1c)

To NX-OS or SAN-OS Release	Nondisruptive Downgrade Path and Ordered Downgrade Steps
NX-OS:	
Release 4.1(1b)	1. Downgrade to NX-OS Release 4.1(x).
SAN-OS:	
All 3.3(x) releases	2. Downgrade to NX-OS Release 4.1(x). 3. Downgrade to SAN-OS Release 3.3(x).
All 3.2(x), 3.1(x), 3.0(x) releases, and all 2.1(x) releases.	1. Downgrade to NX-OS Release 4.1(x). 2. Downgrade to SAN-OS Release 3.3(x). 3. Downgrade to SAN-OS Release 3.2(x), Release 3.1(x)., Release 3.0(x), or Release 2.1(x).

Table 14 Nondisruptive Downgrade Path from NX-OS Release 4.1(1c) (continued)

To NX-OS or SAN-OS Release	Nondisruptive Downgrade Path and Ordered Downgrade Steps
All 2.0(x) releases.	1. Downgrade to NX-OS Release 4.1(x). 2. Downgrade to SAN-OS Release 3.3(x). 3. Downgrade to SAN-OS Release 2.1(2x). 4. Downgrade to SAN-OS Release 2.0(x).
Release 1.x	1. Downgrade to NX-OS Release 4.1(x). 2. Downgrade to SAN-OS Release 3.3(x). 3. Downgrade to SAN-OS Release 2.1(2b). 4. Downgrade to SAN-OS Release 1.3(4a). 5. Downgrade to SAN-OS Release 1.x.

FICON Downgrade Paths

Cisco MDS NX-OS Release 4.1(1c) supports FICON.

Find the image release number that you want to downgrade to in the To SAN-OS Release with FICON Enabled column of the table and follow the recommended downgrade path.

Table 15 FICON Downgrade Path from NX-OS Release 4.1(1c)

To SAN-OS Release with FICON Enabled	Downgrade Path
SAN-OS 3.3(1c)	You can nondisruptively downgrade directly from NX-OS Release 4.1(1c).
SAN-OS 3.2(2c)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.2(2c).
SAN-OS 3.0(3b)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.0(3b).
SAN-OS 3.0(2)	First downgrade to SAN-OS Release 3.3(1c) and then downgrade to Release 3.0(2).
SAN-OS 2.0(2b)	Use the **interface shutdown** command to administratively shut any Fibre Channel ports on Generation 1 modules that are in an operationally down state before nondisruptively downgrading from NX-OS Release 4.1 to SAN-OS Release 3.3(1c) then to SAN-OS Release 3.0(3b) or SAN-OS Release 3.0(2), and then to SAN-OS Release 2.0(2b). An operationally down state includes `Link failure or not-connected, SFP not present`, or `Error Disabled` status in the output of a **show interface** command. When an interface is administratively shut it will then show as `Administratively down`. Interfaces that are currently up or trunking do not need to be shut down.
SAN-OS 1.3(4a)	Downgrade to SAN-OS Release 3.3(1c) and then to Release 3.0(2). Use the shutdown command to shut all the ports operationally down and administratively up on all the Generation 1 modules before nondisruptively downgrading to Release 2.0(2b) and then downgrade to 1.3(4a).

Downgrading from NX-OS 4.x to SAN-OS 3.x

If you need to downgrade from an NX-OS 4.x image to a SAN-OS 3.x image, make sure that you enter the s**ystem health check bootflash** command on the switch running NX-OS 4.x before you downgrade to SAN-OS 3.x. The s**ystem health check bootflash** command, which is available starting in NX-OS 4.1(1b), ensures that the available free space is taken into account properly.

MDS 9100 and 9200 Series Switches

Before downgrading from an NX-OS 4.x image to a SAN-OS 3.x image on an MDS 9100 or 9200 Series switch, follow these steps:

1. Telnet to the switch to be downgraded and log in.
2. Enter the s**ystem health check bootflash** command.

   The following example shows this command and its output:

```
switch# system health check bootflash
NOTE: This command can take over 30 minutes. Bootflash will be offline during th
is time.
Do you want to continue? (yes/no)  [n] y
Unmount successful. Checking bootflash ... please be patient
```

   Although the switch indicates that the bootflash check takes 30 minutes, it typically completes in just a few seconds.
3. Once the bootflash check is complete, proceed with the downgrade process.

MDS 9500 Series Switches

Before downgrading from an NX-OS 4.x image to a SAN-OS 3.x image on an MDS 9500 Series switch, follow these steps:

1. Telnet to the switch to be downgraded and log in.
2. Enter the s**ystem health check bootflash** command.

   The following example shows this command and its output:

```
switch# system health check bootflash
NOTE: This command can take over 30 minutes. Bootflash will be offline during th
is time.
Do you want to continue? (yes/no)  [n] y
Unmount successful. Checking bootflash ... please be patient
```

   Although the switch indicates that the bootflash check takes 30 minutes, it typically completes in just a few seconds.

   Once the bootflash check is complete on the active supervisor, the bootflash on the standby supervisor must be checked.
3. Enter the **show module** command to determine the module number of the standby supervisor. The following example shows that the standby supervisor is module 8.

```
switch# show module
Mod  Ports  Module-Type                       Model              Status
---  -----  --------------------------------- ------------------ ------------
4    32     Storage Services Module           DS-X9032-SSM       ok
5    16     2x1GE IPS, 14x1/2Gbps FC Module   DS-X9302-14K9      ok
7    0      Supervisor/Fabric-2               DS-X9530-SF2-K9    active *
8    0      Supervisor/Fabric-2               DS-X9530-SF2-K9    ha-standby
10   22     4x1GE IPS, 18x1/2/4Gbps FC Modul  DS-X9304-18K9      ok
```

4. Enter the **attach module** command to attach to the standby supervisor module number shown in the output of the **show module** command, and then enter the **system health check bootflash** command.

```
switch# attach module 8
Attaching to module 8 ...
To exit type 'exit', to abort type '$.'
Cisco Nexus Operating System (NX-OS) Software
……
Switch(standby)# system health check bootflash
NOTE: This command can take over 30 minutes. Bootflash will be offline during th
is time.
Do you want to continue? (yes/no) [n] y
Unmount successful. Checking bootflash ... please be patient
```

Although the switch indicates that the bootflash check takes 30 minutes, it typically completes in just a few seconds.

Once the bootflash check is complete on both the active and the standby supervisors, proceed with the downgrade process.

Note The s**ystem health check bootflash** command is available starting in NX-OS 4.1(1b).

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 NX-OS Release 4.1 to any SAN-OS 2.x release earlier than SAN-OS Release 2.1(2e). Power down the SSM and perform the downgrade. Bring up the SSM with the new bootvar set to the 2.x SSI image.
- Downgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*.
- SSM intelligent services traffic switching on SSM ports is disrupted on upgrades or downgrades.
- Fibre Channel switching traffic on SSM ports is not disrupted under the following conditions:
  - All SSM applications are disabled. Use the **show ssm provisioning** command to determine if any applications are provisioned on the SSM. Use the **no ssm enable feature** configuration mode command to disable these features.
  - The EPLD version on the SSM is at 0x07 or higher. Use the **show version module** *slot* **epld** command to determine your EPLD version. Refer to the *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images* to upgrade your EPLD image.
  - Refer to the *Cisco Data Center Interoperability Support Matrix* and the "Managing Modules" chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x,* for information on downgrading your SSM.

New Features in Cisco MDS NX-OS Release 4.1(1c)

This section briefly describes the new features introduced in this release.

Cisco MDS NX-OS Release 4.1(1c) is a FICON certified version of Cisco MDS NX-OS Release 4.1(1b). For a complete list of the features in NX-OS Release 4.1(1b), see the *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS 4.1(1b)*. 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 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 NX-OS and SAN-OS documentation set, see the "Related Documentation" section.

Licensed Cisco NX-OS Software Packages

Most Cisco MDS 9000 family software features are included in the base configuration of the switch: the standard package. However, some features are logically grouped into add-on packages that must be licensed separately, such as the Cisco MDS 9000 Enterprise package, SAN Extension over IP package, Mainframe package, Fabric Manager Server (FMS) package, Storage Services Enabler (SSE) package, Storage Media Encryption package, and Data Mobility Manager package. On-demand ports activation licenses are also available for the Cisco MDS Blade Switch Series, and 4-Gbps Cisco MDS 9100 Series Multilayer Fabric Switches.

Enterprise Package

The standard software package that is bundled at no charge with the Cisco MDS 9000 Family switches includes the base set of features that Cisco believes are required by most customers for building a SAN. The Cisco MDS 9000 family also has a set of advanced features that are recommended for all enterprise SANs. These features are bundled together in the Cisco MDS 9000 Enterprise package. Refer to the Cisco MDS 9000 Enterprise package fact sheet for more information.

SAN Extension over IP Package

The Cisco MDS 9000 SAN Extension over IP package allows the customer to use FCIP to extend SANs over wide distances on IP networks using the Cisco MDS 9000 family IP storage services. Refer to the Cisco MDS 9000 SAN Extension over IP package fact sheet for more information.

Mainframe Package

The Cisco MDS 9000 Mainframe package uses the FICON protocol and allows control unit port management for in-band management from IBM S/390 and z/900 processors. FICON VSAN support is provided to help ensure true hardware-based separation of FICON and open systems. Switch cascading, fabric binding, and intermixing also are included in this package. Refer to the Cisco MDS 9000 Mainframe package fact sheet for more information.

Fabric Manager Server Package

The standard Cisco Fabric Manager and Device Manager applications bundled at no charge with the Cisco MDS 9000 family provide basic configuration and troubleshooting capabilities. The Cisco MDS 9000 FMS package extends Cisco Fabric Manager by providing historical performance monitoring for network traffic hotspot analysis, centralized management services, and advanced application integration for greater management efficiency. Refer to the Cisco MDS 9000 FMS package fact sheet for more information.

Storage Services Enabler Package

The Cisco MDS 9000 SSE package allows network-based storage applications and services to run on the Cisco MDS 9000 family SSMs, Cisco MSM-18/4 Port Multiservice Module, and Cisco MDS 9222i. Intelligent fabric applications simplify complex IT storage environments and help organizations gain control of capital and operating costs by providing consistent and automated storage management. Refer to the Cisco MDS 9000 SSE package fact sheet for more information.

On-Demand Port Activation License

On-demand ports allow customers to benefit from Cisco NX-OS Software features while initially purchasing only a small number of activated ports on 4-Gbps Cisco MDS 9100 Series Multilayer Fabric Switches. As needed, customers can expand switch connectivity by licensing additional ports.

Storage Media Encryption Package

The Cisco MDS 9000 Storage Media Encryption package enables encryption of data at rest on heterogeneous tape devices and virtual tape libraries as a transparent fabric service. Cisco SME is completely integrated with Cisco MDS 9000 Family switches and the Cisco Fabric Manager application, enabling highly available encryption services to be deployed without rewiring or reconfiguring SANs, and allowing them to be managed easily without installing additional management software. Refer to the Cisco MDS 9000 Storage Media Encryption package fact sheet for more information.

Data Mobility Manager Package

The Cisco MDS 9000 Data Mobility package enables data migration between heterogeneous disk arrays without introducing a virtualization layer or rewiring or reconfiguring SANs. Cisco DMM allows concurrent migration between multiple LUNs of unequal size. Rate-adjusted migration, data

verification, dual Fibre Channel fabric support, and management using Cisco Fabric Manager provide a complete solution that greatly simplifies and eliminates most downtime associated with data migration. Refer to the Cisco MDS 9000 Data Mobility Manager package fact sheet for more information.

Limitations and Restrictions

This section lists the limitations and restrictions for this release. The following limitations are described:

IPv6

The management port on Cisco MDS switches supports one user-configured IPv6 address, but does not support auto-configuration of an IPv6 address.

User Roles

In SAN-OS Release 3.3(x) and earlier, when a user belongs to a role which has a VSAN policy set to Deny and the role allows access to a specific set of VSANs (for example, 1 through 10), the user is restricted from performing the **configuration**, **clear**, **execute**, and **debug** commands which had a VSAN parameter outside this specified set. Beginning with NX-OS Release 4.1(1b), these users are still prevented from performing **configuration**, **clear**, **execute**, and **debug** commands as before, however, they are allowed to perform **show** commands for all VSANs. This addresses the following:

1. In a network environment, users often need to view information in other VSANs even though they do not have permission to modify configurations in those VSANs.
2. This makes the Cisco MDS behavior consistent with other Cisco products such as Nexus 7000 which exhibits the same behavior for those roles (when they apply to the VLAN policy).

Data Mobility Manager

For a storage-based Data Mobility Manager (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. For scheduled DMM jobs, make sure all server HBA ports and storage ports (both existing and new storage) are up.

Red Hat Enterprise Linux

The Linux kernel core dump is not supported in NX-OS Release 4.1(1c) and later versions and therefore the CLI command has been removed. A syntax error message will be displayed if you import configurations from SAN-OS Release 3.3(x) and earlier to NX-OS Release 4.1(1c) and later. These syntax errors do not affect the application of other commands in the configuration and can be safely ignored. To address this, remove the kernel core configuration from the ASCII configuration file before importing the configuration.

Generation 1 Module Limitation

When a Cisco or other vendor switch port is connected to a Generation 1 module port (ISL connection), the receive buffer-to-buffer credit of the port connected to a Generation 1 module port should not exceed 255.

Schedule Job Configurations

In Cisco MDS NX-OS Release 4.1(1c) and later the scheduler job configurations need to be entered in a single line with a semicolon(;) as the delimiter.

Job configuration files created with SAN-OS Release 3.3(1c) and earlier, are not supported. However, you can edit the job configuration file and add the delimiter to support Cisco NX-OS Release 4.1(1c).

Solaris Windows Manager

Solaris Windows Manager does not resize windows correctly which effects some Device Manager screens. To resolve this, download and install the 119538-1 patch from Sun Microsystems. The patch (119538-17 GNONE 2.6.0: Windows Manager Patch, Generic, 2008/08/08) can be obtained from sunsolve.sun.com.

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.

InterVSAN Routing

When using InterVSAN Routing (IVR), it is recommended to enable Cisco Fabric Services (CFS) on all IVR-enabled switches. Failure to do so may cause mismatched active zone sets if an error occurs during zone set activation.

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 NX-OS Release 4.1(1c) 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.

Applying Zone Configurations to VSAN 1

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

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

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

Running Storage Applications on the MSM-18/4

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

Compatibility of Fabric Manager and Data Mobility Manager

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

PPRC Not Supported with FCIP Write Acceleration

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

Caveats

This section lists the open and resolved caveats for this release. Use Table 16 to determine the status of a particular caveat. In the table, "O" indicates an open caveat and "R" indicates a resolved caveat.

Table 16 Open Caveats and Resolved Caveats Reference

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	4.1(1b)	4.1(1c)
Severity 1		
CSCsv20465	O	O
CSCsv66455	O	R
Severity 2		
CSCsk11207	O	O
CSCsq78868	O	O
CSCsu33302	O	O
CSCsu98190	O	O
CSCsv15022	O	R
CSCsv27564	O	O
CSCsv57351	O	R
CSCsv83063	O	R
CSCsw95386	O	O
CSCsz59152	O	O
CSCsz84411	—	O
CSCtb00005	O	O
CSCtb28442	O	O
CSCtb77695	O	O
CSCtc20849	O	O
CSCtc48338	O	O
CSCtd16646	O	O
Severity 3		
CSCsk35725	O	O
CSCsk49309	O	O
CSCsm47252	O	O
CSCsq20408	O	O
CSCsr69166	O	O
CSCsu23984	O	O
CSCsu30034	O	O
CSCsu39975	O	O

Table 16 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	NX-OS Software Release (Open or Resolved)	NX-OS Software Release (Open or Resolved)
	4.1(1b)	4.1(1c)
CSCsu53299	O	O
CSCsu63218	O	O
CSCsu72195	O	O
CSCsu73264	O	O
CSCsu84511	O	O
CSCsu87264	O	O
CSCsu88059	O	O
CSCsv52710	O	R
CSCsz01738	O	O
CSCtc04286	O	O
Severity 4		
CSCsv10493	O	R
CSCsy23429	O	O

Resolved Caveats

- CSCsv66455

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

  Workaround: This issue is resolved.

- CSCsv15022

  Symptom: When a port member is added to or deleted from a PortChannel and lossless in-order delivery (LIOD) is in effect, sometimes the LIOD transaction (adding or deleting the port member) might take more than 500 milliseconds to complete if there is a heavy traffic load on an MDS 8-Gbps Fibre Channel switching module. As a result, packets might time out on the switch and drop. By default, in-order delivery is enabled for the FICON VSAN only.

  Workaround: This issue is resolved.

- CSCsv57351

  Symptom: In Cisco NX-OS Release 4.1(1b), intermittent packet drops are observed in SME with large restores, especially with large and bursty I/Os.

  Workaround: This issue is resolved.

- CSCsv83063

  Symptom: With SSL enabled between the switches and the Key Management Center (KMC), the transport comes up with a delay at times. This causes key lookup timeout errors to occur.

  Workaround: This issue is resolved.

- CSCsv52710

  Symptom: In rare cases, it is possible for SFPs connected to Gigabit Ethernet interfaces to not be detected on a reload of a module. This applies to MDS 9222i and MSM-18/4 modules.

  Workaround: This issue is resolved.

- CSCsv10493

  Symptom: Under certain conditions, the software can detect that the NVRAM has failed and a syslog is generated indicating that NVRAM has failed. The following message is displayed:

  ```
  %SYSTEMHEALTH-2-OHMS_NVRAM_FAILED: Nvram test maximum failures reached for module 7
  for blocks 0x1000.
  ```

  There is no impact to the system because this happens to a block that is unused.

  Workaround: This issue is resolved.

Open Caveats

- CSCsv20465

  Symptom: High mgmt0 traffic rates (such as a during a broadcast storm) may cause a supervisor 2 type switch to reload.

  Workaround: None.

- CSCsk11207

  Symptom: Using Fabric Manager Web Client, you download Fabric Manager Client and when prompted to create a desktop shortcut, you select Yes. The default shortcut named "Cisco Fabric Manager" is created on the desktop. Then, using Fabric Manager Web Client again, you download another Fabric Manager Client from a different server (usually this will be a different version of Fabric Manager Client). You will not be prompted to create another shortcut because a desktop shortcut titled "Cisco Fabric Manager" already exists from the first installation.

  Workaround. To create multiple Fabric Manager Client desktop shortcuts with unique names, follow these steps:

  1. From **Start > Control Panel > Java > Temporary Internet Files >** click **View**. The Java Cache Viewer is launched.
  2. Right-click one of the versions of Fabric Manager Client and select **Install Shortcuts** from the drop down menu. The shortcut is created on the desktop.
  3. Change the name of the new shortcut.
  4. Repeat Steps 2 and 3 for each additional Fabric Manager Client.

- 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 a PortChannel instead of multiple links to achieve more bandwidth.

- CSCsu33302

  Symptom: An upgrade from NX-OS Release 4.1(1x) to NX-OS Release 4.2(1) might fail if the NX-OS Release 4.2(1) image takes longer to fully boot up than the time allocated by NX-OS Release 4.1(1x). If this occurs, you might see the following message:

  ```
  2009 Jul 28 10:29:56 emc-Fc-vegas2 %KERN-2-SYSTEM_MSG: mts_tcp_client_init():
  ret=-115, TCP HA SYNC connection to Standby Supervisor failed. Sock state=2,
  sk->state=1 - kernel
  2009 Jul 28 10:29:56 emc-Fc-vegas2 %KERN-2-SYSTEM_MSG: TCP connection to Standby
  failed with rc -115 - kernel
  ```

  The upgrade will abort and the standby supervisor will reload with the NX-OS Release 4.1(1x) image.

  Workaround: After the switch returns to the state prior to the upgrade where both the active and standby supervisors are running NX-OS Release 4.1(1x), enter the **install all** command to try the upgrade again.

- CSCsu98190

  Symptom: During an upgrade from Cisco MDS SAN-OS Release 3.3(1c) to Cisco NX-OS 4.1(1b) and later, applications might experience a very small amount of packet drops in the fabric. Most of the applications should be able to recover from such a small packet loss. The problem is seen only with an upgrade from SAN-OS Release 3.3(1c) and is not seen with an upgrade from either SAN-OS Release 3.3(1a) or SAN-OS Release 3.3(1b).

  Workaround: Before starting the ISSU from SAN-OS Release 3.3(1c), follow these steps:

1. Enter the **no ntp drop-aged-packet** command.
2. Enter the **sh ntp timestamp-status** command to verify that the command executed successfully. The output should display the following message:

```
Timestamp has been disabled through CLI
```

Note When the **no ntp drop-aged-packet** command is in effect, aged packets due to congestion are not dropped. If you cannot perform the ISSU after entering the command, revert back to enable the timestamp check by entering the **ntp drop-aged-packet** command.

- CSCsv27564

  Symptom: In rare cases, following a downgrade from an NX-OS 4.x image to a SAN-OS 3.x image, the available space on the bootflash might be displayed as less than the actual space that is available.

  Workaround: Before downgrading from an NX-OS 4.x image to a SAN-OS 3.x image, enter the **system health check bootflash** command, which is available starting in NX-OS 4.1(1b), to ensure that the available free space is taken into account properly. The following example shows this command and its output:

```
switch# system health check bootflash
NOTE: This command can take over 30 minutes. Bootflash will be offline during th
is time.
Do you want to continue? (yes/no)  [n]
```

  Although the switch indicates that the bootflash check takes 30 minutes, it typically completes in just a few seconds.

  Once the bootflash check is complete, you can proceed with the downgrade process.

Note If you are downgrading an MDS 9500 Series switch, you must enter the **system health check bootflash** command on both the active supervisor and the standby supervisor. You will need to enter the **show module** command to determine the standby module and then attach to that module by entering the **attach module** command. For detailed instructions, see the "Downgrading from NX-OS 4.x to SAN-OS 3.x" section on page 31.

- 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.

- CSCsz59152

  Symptom: On an MDS 9513 switch, the crossbar ASIC on a Fabric 1 or Fabric 2 module may fail. As a result, some ports may get disabled on the modules that use the crossbar links in the bad fabric module.

  Workaround: To resolve this issue, follow these steps:

  1. Replace the affected Fabric 1 or Fabric 2 module.
  2. Manually bring up the ports that went down by entering the **shut** command, followed by the **no shut** command.

- CSCsz84411

  Symptom: An MDS 9124 switch may randomly reboot with a reset reason of unknown. This is a rare event and occurs only in systems that have a single power supply with a serial number beginning with QCS.

  Workaround: Install and power up the redundant power supply.

- CSCtb00005

  Symptom: On an MDS 9000 switch running NX-OS Release 4.1(x) software, if three supervisor switchovers occur within a 20-minute period, an embedded event manager (EEM) policy triggers the power down of all modules in the chassis. Internal processing associated with the EEM policy might leave the state of a module out-of-sync with the supervisor module.

  Workaround: Remove the module and then reinstall it.

- CSCtb28442

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

  Workaround: None.

- CSCtb77695

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

  Workaround: None.

- CSCtc20849

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

```
switch# show cores
Module-num       Process-name      PID     Core-create-time
----------       ------------      ---     ----------------
8                qos               15671   Sep 21 22:16
7                qos               4370    Sep 21 22:17

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

----- reset reason for Supervisor-module 7 (from Supervisor in slot 7) ---
1) At 260648 usecs after Mon Sep 21 22:12:37 2009
```

```
Reason: Reset triggered due to HA policy of Reset
Service: Service "qos"
Version: 3.3(2)
```

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

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

- CSCtc48338

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

  - **show hardware internal mgmt0 stats**
  - **show hardware internal eobc stats**
  - **show tech**
  - **show tech details**
  - **show tech-support**
  - **tac-pac**

  In NX-OS Release 4.1(x) and Release 4.2(x), there are two additional commands that may cause this issue:

  - **show tech-support sysmgr**
  - **show tech-support ha**

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

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

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

  - Do not enter the **show hardware internal mgmt0 stats** command or the **show hardware internal eobc stats** command.
  - Upgrade to one of the following software releases when it becomes available:

    Cisco SAN-OS Release 3.3(4a) or above

    Cisco NX-OS Release 4.2(3) or above
  - Before running the **show tech-support** command, the **show tech-support details** command, or the **tacpac** command from the CLI or from Cisco Fabric Manager or Device manager, download a plug-in from the Software Download Center to patch the commands. Load the plug-in on the active and standby supervisor as described in the following steps. The plug-in is not persistent across switchovers and should be loaded any time a switchover occurs.

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

  1. Download the plug-in from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=282764109
  2. Select release 1.0.

3. Make a copy of the downloaded gplug by entering the following command:
   switch# copy bootflash:m9500-sup2-showtech-FN63288-plugin-1.0.bin bootflash:gplug_copy
4. Copy the copy of the gplug to the standby supervisor by entering the following command:
   switch# **copy bootflash:gplug_copy bootflash://sup-remote/**
5. Load the gplug on the active supervisor by entering the following command:
   switch# **load bootflash:gplug_copy**
6. Attach to the standby supervisor by entering the following command:
   switch# **attach module** <standby-sup-slot>
7. Load the gplug onthe standby supervisor by entering the following command:
   switch# **load bootflash:gplug_copy**

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

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

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

- CSCtd16646

  Symptom: Bit errors occurred on frames received from the Cisco Fabric Switch for IBM BladeCenter on slots 1 through 4.

  Workaround: Upgrade to NX-OS Relase 4.2(3) where this issue is resolved.

- 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.

- CSCsk49309

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

  Workaround: None.

- 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 Modules (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 reestablished in time, the DMM jobs in that SMM will move to the Reset state.

  Workaround: None.

- CSCsq20408

  Symptom: The **show startup** command displays aspects of the running configuration file when SANtap is configured and/or SANtap objects are created. When a user creates objects, such as a CVT or DVT, the configuration is showing in the running-configuration file and in the startup-configuration file without copying the configuration into the startup-configuration file.

  Workaround: Use the **copy running-config startup-config** command whenever you create objects such as a CVT or DVT so that the running-configuration and startup-configuration are synchronized.

- CSCsr69166

  Symptom: Solaris Windows Manager does not resize windows correctly which affects some Device Manager screens.

  Workaround: Download and install the 119538-1 patch from Sun Microsystems. The patch (119538-17 GNONE 2.6.0: Windows Manager Patch, Generic, 2008/08/08) can be obtained from sunsolve.sun.com.

- CSCsu23984

  Symptom: Starting with MDS NX-OS 4.1(1), a password security feature allows a user to enable a secure password standard. However, this feature is not being enforced for SNMP users.

  Workaround: None.

- CSCsu30034

  Symptom: During an In-Service Software Upgrade (ISSU), throughput statistics will not be available from the switch undergoing an upgrade. This information will not be able available from the CLI or Device Manager via SNMP.

  Workaround: After the upgrade is complete, the statistics will become available.

- CSCsu39975

  Symptom: Device Manager does not install and the system displays this error:

  ```
  [ERROR] no !/ in spec
  ```

  This issue occurs in Fabric Manager and Device Manager Release 3.2(x), Release 3.3(x), Release 3.4(x), and Release 4.1(x).

  Workaround: Uninstall JRE 1.5_16 and install any other JRE 1.5 update if you intend to use Device Manager Release 3.2(x). Use JRE 1.6 with Device Manager Release 3.3(x), Release 3.4(x), and Release 4.1(x).

- CSCsu53299

  Symptom: When reloading a switch, a timing condition may cause CFS to enter the handshake before the Routing Information Base (RIB) does. In this instance, CFS will not see any peers, and CFS-based applications will not communicate with the rest of the fabric.

  Workaround: Reinitialize CFS by using the following commands. Reinitialization will cause CFS to reattempt the query to RIB.

  ```
  switch-1#   configure terminal
  switch-1#   no cfs distribute
  switch-1#   cfs distribute
  ```

- CSCsu63218

  Symptom: In some cases, there may be duplicate entries of a global pWWN and virtual pWWN as identified in the following scenarios:

  Switch 1 has a v1 and p1 entry, and p1 is connected to one of the server interfaces on switch 1.

  Switch 2 also has a v1 and p1 entry, with a v2 and p2 entry. Switch 2 is in a different CFS region.

  While using the Replace function on different switch options in the FA wizard, if v1 and p2 are provided in Step 4, then expected operations will not be performed.

  Workaround: Use the CLI or Device Manager to remove one duplicate entry and then run the wizard again.

- CSCsu72195

  Symptom: When replaying DMM job configurations that are saved as an ASCII text file (after performing a write erase), the DMM job includes discrepancies that occur due to the interface and zone configurations that are in an area below the DMM job configuration in the ASCII text file. The configurations stored in the ASCII text file are replayed sequentially from top to bottom.

  Workaround: None.

- CSCsu73264

  Symptom: Data Mobility Manager (DMM) uses VSAN 1 for IP communication and it requires **interface cpp** *module***/1/1** to be configured. If another CPP IP Fibre Channel interface is configured in the same module in a different VSAN, then DMM will not work.

  Workaround: Delete both CPP IP Fibre Channel interfaces and create only one interface in VSAN 1.

- CSCsu84511

  Symptom: When a Cisco MDS switch is configured to use an AAA server using TACACS+ and the directed request option is enabled, a login using <user>@<server> provides the network-operator privilege instead of the actual privilege mentioned in the ACS server. This problem occurs once AAA accounting is set to remote. A login without the directed request option enabled works as expected and provides the appropriate privilege. This problem does not occur when using the RADIUS protocol with the directed request option enabled.

  Workaround: Use the RADIUS protocol with the directed request option enabled.

- CSCsu87264

  Symptom: The Cisco MDS 9000 Family 1/2/4/8-Gbps 24-Port FC Module (DS-X9224-96K9) and the Cisco MDS 9000 Family 1/2/4/8-Gbps 48-Port FC Module (DS-X9248-96K9) go to the OK state when plugged into a Cisco MDS 9216i switch. The MDS 9216i switch does not support these two modules in NX-OS Release 4.1(1b).

  Workaround: Do not use these unsupported modules in the MDS 9216i switch.

- CSCsu88059

  Symptom: After first installing Fabric Manager Server (FMS) (with default flag displayFCoE = false), and then stopping and restarting the FMS with displayFCoE = true, the FCoE interface tables are not showing when the old disconnected client reconnects. As a result, the following four FCoE menus do not launch the corresponding tables (FCOE, Virtual Interface Group, Virtual FC Interfaces, and Virtual Ethernet Interfaces).

  Workaround: Close the original Fabric Manager Client and start a new client for the same fabric. The new client will be able to launch all four menus listed above.

- 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.

- CSCtc04286

  Symptom: During bring up of the switch port, the port may go into an error disabled state with the reason “excessive interrupts.” This situation can occur if the other end that is connected to the port continuously sends OLS or NOS primitives.

Workaround: To recover from the failure, enter the **shut** command, followed by the **no shut** command for the port. The switch will attempt to bring up the port again

- CSCsy23429

  Symptom: Cross site scripting (XSS) issues exist in Fabric Manager Server when the Microsoft Internet Explorer web browser is used for web client management.

  Workaround: None.

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*
- *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

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.