Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Release 4.2(7a)

Release Date: August 23, 2010

Part Number: OL-19964-08 K0

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 51.

This document also contains upgrading guidelines that are specific to upgrading to Cisco MDS NX-OS Release 4.2(7a). Before you begin the upgrade process, read the instructions in the "Guidelines for Upgrading to NX-OS Release 4.2(7a)" section on page 16.

Note As of Cisco Fabric Manager Release 4.2(1a), Fabric Manager information will no longer appear in the Cisco MDS 9000 Family Release Notes for NX-OS releases. Cisco Fabric Manager Release Notes will include information that is exclusive to Fabric Manager as a management tool for Cisco MDS 9000 Family switches and Cisco Nexus 5000 Series switches. Refer to the following website for Release Notes for Cisco Fabric Manager:
http://www.cisco.com/en/US/products/ps10495/prod_release_notes_list.html

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 on-line change history for this document.

Table 1 Online History Change

Revision	Date	Description
A0	08/23/2010	Created release notes.
B0	09/21/2010	Updated the description of the Slow Drain feature in the "New Features in Cisco MDS NX-OS Release 4.2(7a)" section to include the hardware components that do not support the feature.

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

Table 1 Online History Change

Revision	Date	Description
C0	10/08/2010	Corrected the caveat number of DDTS CSCtc65411to DDTS CSCtc65441.
D0	02/09/2011	Updated the "Licensed Cisco NX-OS Software Packages" section.
E0	03/11/2011	Added the "Slow Drain Feature is On Following Upgrade" topic to the "Guidelines for Upgrading to NX-OS Release 4.2(7a)" section. Added a note stating that the slow drain feature is enabled by default to the "New Features in Cisco MDS NX-OS Release 4.2(7a)" section.
F0	04/29/2011	• Updated the upgrade path to Release 4.2(7a) from 4.1(1x) releases in Table 10. • Added DDTS CSCtn68418 as an Open Caveat. • Added DDTS CSCto68011 as an Open Caveat.
G0	05/11/2011	Corrected the upgrade path to Release 4.2(7a) in Table 10.
H0	09/09/2011	Added the "Configuring a Persistent FCID in an IVR Configuration with Brocade Switches" section.
I0	03/11/2012	Updated Table 10 and Table 13.
J0	05/03/2012	• Updated Table 10. • Added open caveat CSCty32238.
K0	05/18/2012	Added the "Converting Automatically Created PortChannels Before an Upgrade" section.

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	M95S2K9-4.2.7a	MDS 9500 Supervisor/Fabric-2, NX-OS software	MDS 9500 Series only
	M92S2K9-4.2.7a	MDS 9200 Supervisor/Fabric-2, NX-OS software	MDS 9222i Switch only
	M92S1K9-4.2.7a	MDS 9216i Supervisor/Fabric-I, NX-OS software	MDS 9216i Switch only
	M91S2K9-4.2.7a	MDS 9100 Supervisor/Fabric-2, NX-OS software	MDS 9124 Switch and MDS 9134 Switch
SSI Interface	SSI-M9K9-427a	Storage Services Interface for NX-OS Release 4.2(7a)	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

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

Component	Part Number	Description	Applicable Product
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
	M92SSESSNK9	Cisco Storage Services Enabler License for SSN-16 (1 engine)	MDS 9200 Series only
	M95SSESSNK9	Cisco Storage Services Enabler License for SSN-16 (1 engine)	MDS 9500 Series only
	M92SMESSNK9	Cisco Storage Media Encryption License for SSN-16 (1 engine)	MDS 9200 Series only
	M95SMESSNK9	Cisco Storage Media Encryption License for SSN-16 (1 engine)	MDS 9500 Series only
	M92IOASSN	Cisco I/O Accelerator License for SSN-16 (1 engine)	MDS 9200 Series only
	M95IOASSN	Cisco I/O Accelerator License for SSN-16 (1 engine)	MDS 9500 Series only
	M92IOA184	Cisco I/O Accelerator License for MSM-18/4	MDS 9200 Series only
	M95IOA184	Cisco I/O Accelerator License for MSM-18/4	MDS 9500 Series only
	M9222IIOA	Cisco I/O Accelerator License for Cisco MDS 9222i base switch	MDS 9222i Switch only
	M92EXTSSNK9	Cisco SAN Extension License for SSN-16 (1 engine)	MDS 9200 Series only
	M95EXTSSNK9	Cisco SAN Extension License for SSN-16 (1 engine)	MDS 9500 Series only
	M9200XRC	Cisco XRC Acceleration	MDS 9200 Series only
	M9500XRC	Cisco XRC Acceleration	MDS 9500 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-X9316-SSNK9	Cisco MDS 9000 Family 16-Port Storage Services Node (SSN-16) — 16 fixed 1-Gbps Ethernet ports, plus 4 service engines that support 4 Gigabit Ethernet IP storage services ports.	MDS 9500 Series MDS 9222i Switch
	DS-X9304-18K9	Cisco MDS 9000 18/4-Port Multiservice Module (MSM-18/4) — 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	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 9134	Yes
MD S 9124	Yes
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-2 Module	Yes	N/A	N/A
DS-X9530-SF2A-K9	MDS 9500 Supervisor-2A Module	Yes	N/A	N/A
DS-X9530-SF1-K9	MDS 9500 Supervisor-1 Module	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	Yes
DS-X9316-SSNK9	16-port Storage Services Node (SSN-16)	Yes	Yes	No
DS-X9304-18K9	18/4-Port Multiservice 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
DS-X9016	16-port 1-, 2-Gbps Fibre Channel Switching 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-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-SF2A-K9	MDS 9500 Supervisor-2A 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-X9316-SSNK9	16-port Storage Services Node (SSN-16)	No	No	No	No	No
DS-X9304-18K9	18/4-Port Multiservice 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 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*.

Supervisor-2A Module

The Cisco MDS 9500 Series Supervisor-2A module, DS-X9530-SF2A-K9, is a new supervisor module for the Cisco MDS 9500 Series. The Supervisor-2A module is functionally equivalent to the Supervisor-2 module, but has these distinguishing features:

- The Supervisor-2A module supports the deployment of Fibre Channel over Ethernet (FCoE) in the MDS 9500 Multilayer Director Chassis
- The Supervisor-2A module has 2 GB of memory, twice that of the Supervisor-2 module

For additional information about the Supervisor-2A module, see the *Cisco MDS 9500 Series Supervisor-2A Tech Note*.

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.

Determining Software Version Compatibility

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

Table 6 Software Release Compatibility

NX-OS Software	Minimum NX-OS Release	Tested NX-OS Release
NX-OS Release 4.2(7a)	SAN-OS Release 3.3(1c) or later	SAN-OS Release 3.3(1c), 3.3(5)
	NX-OS Release 4.1(1b) or later	NX-OS Releases 4.1(1b), 4.2(5)

Fabric Manager Software	Minimum NX-OS Release	Tested NX-OS Releases
Fabric Manager Release 4.2(7a)	SAN-OS Release 3.3(1c) or later	NX-OS Release 3.3(1c), 3.3(5)
	NX-OS Release 4.1(1b) or later	NX-OS Release 4.1(1b), 4.2(5), 4.2(7a)

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 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

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 Cisco MDS NX-OS Release 4.2(7a) supports. See the "MDS 9000 Chassis and Module Support in Cisco MDS NX-OS 4.x" section on page 10.

For detailed instructions for performing a software upgrade using Cisco Fabric Manager, see the *Cisco Fabric Manager Release Notes for Release 4.2(1a)*, which is available from the following website:

http://www.cisco.com/en/US/products/ps10495/prod_release_notes_list.html

Guidelines for Upgrading to NX-OS Release 4.2(7a)

This section lists guidelines that are specific to upgrading your Cisco MDS NX-OS software image to NX-OS Release 4.2(7a), and includes the following topics:

Slow Drain Feature is On Following Upgrade

Cisco NX-OS Release 4.2(7a) includes the slow drain feature. This new feature is enabled by default, so it is on once you upgrade to Release 4.2(7a). For additional information about this feature and a link to the documentation for it, see the "New Features in Cisco MDS NX-OS Release 4.2(7a)" section on page 31.

Debug Messages Displayed During Upgrade

If you have the port monitor enabled when you upgrade to NX-OS Release 4.2(7a), the following messages are displayed:

```
2010 Jul 19 04:29:16 interop-9509 %PMON-SLOT2-2-PMON_CRIT_INFO: Port Monitor Critical
Information: policy slowdrain invalid,object 1 interval is 0; setting to default 10.
2010 Jul 19 04:29:16 interop-9509 %PMON-SLOT2-2-PMON_CRIT_INFO: Port Monitor Critical
Information: policy slowdrain invalid,object 2 interval is 0; setting to default 10.
```

These debug messages are displayed if you upgrade to an NX-OS release that has slow drain enabled by default, such as NX-OS Release 4.2(7a), from a release that did not have the slow drain feature, such as NX-OS Release 4.2(5). The messages are triggered when a module becomes aware of the new slow drain feature that was not present in NX-OS software prior to NX-OS Release 4.2(7a). These message are harmless and can be ignored.

You should not see these messages when you upgrade from a release that has the slow drain feature to another release that also has the slow drain feature, such as when you upgrade from NX-OS Release 4.2(7x) to Release 5.0(4b).

Upgrading from NX-OS Release 4.2(5) to Release 4.2(7a) with DMM, IOA, or SME Configured

If you plan to upgrade from NX-OS Release 4.2(5) to NX-OS Release 4.2(7a), be aware that in some corner cases, the upgrade might be disruptive if you have one of the following applications configured on your switch: DMM, IOA, or SME.

You can detect this issue by entering the following command:

```
switch#show incompatibility-all system bootflash:isan-427
The following configurations on active are incompatible with  the system image
1) Service : fc-redirect , Capability : CAP_FEATURE_FC_REDIRECT_IVR_SUPPORT_ENABLED
Description : FC-Redirect IVR Support is Enabled
```

```
Capability requirement : STRICT
Disable command : a. FC-Redirect ivr-support is enabled on this switch. This feature
requires all IVR-enabled switches and switches with FC-Redirect based application
nodes to have a NX-OS version that supports the feature.
b. If no FC-Redirect config for IVR flows exists, please disable the feature using
the command 'no fc-redirect ivr-support enable' and try again.
switch#
```

The following corner cases can lead to this issue:

- A switch with active SME or IOA nodes with a IT-Nexus bound to local nodes is upgraded or downgraded to NX-OS Release 4.2(5).
- If a switch running NX-OS Release 4.2(5) is configured as a DMM, IOA, or SME node and it services active flows and one or the other of the following events occurs:
- A system switchover occurs in a dual supervisor system, either through a CLI command entered by a user or because of a HA policy trigger.
- A FC Redirect process fails and restarts.

In both these cases, enter the **show incompatibilities** command to verify if the symptom exists.

The steps for working around this issue depend on your switch configuration and are described in the following sections.

Single Supervisor System

On a single supervisor system, you cannot perform a nondisruptive upgrade or downgrade. You must perform a disruptive upgrade or downgrade. This workaround applies to all the three applications: DMM, IOA, and SME.

Dual Supervisor System

On a dual supervisor system, the workaround is different for each application:

- **DMM**

  Follow these steps:

  1. Delete all DMM jobs.
  2. Enter a **system switchover** command.

- **SME**

  Follow these steps:

  1. Move the SME master node to another SME node in the same cluster and then remove the old SME master node from the SME cluster.

  a. To move the SME master node to another switch, enter the commands as follows:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# sme cluster c1
switch(config-sme-cl)# shutdown
This change can be disruptive. Please ensure you have read the "SME Cluster
Recovery Procedure" in the configuration guide. -- Are you sure you want to
continue? (y/n) [n] y
switch(config-sme-cl)# 2010 Jul 20 17:03:34 sw2-qa05
%CLUSTER-2-CLUSTER_LOCAL_NODE_EXIT: Local
```

```
Node 0x1 has left the Cluster 0x2e3b547fee001f20
switch(config-sme-cl)# show sme cluster c1 node summary
------------------------------------------------------------------------------
Switch                  Status           Master
------------------------------------------------------------------------------
local switch            unknown (cluster is offline)
172.25.245.195          unknown (cluster is offline)
```

b. To remove the old master node from the cluster, enter the following commands on the new SME master node:

```
switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# sme cluster c1
switch(config-sme-cl)# no node 172.25.245.193
switch# show sme cluster c1 node summary
------------------------------------------------------------------------------
Switch                  Status          Master
------------------------------------------------------------------------------
local switch            online          yes
```

2. Enter the **system switchover** command on the switch:

```
switch# system switchover
```

3. When the standby supervisor comes back up after the switchover, perform a nondisruptive upgrade or downgrade to the target NX-OS release on the switch. Then enter the following command:

```
switch# show incompatibility-all system bootflash:isan-427
No incompatible configurations
```

4. Once the upgrade is complete, you can add this upgraded node to the SME cluster.

```
switch(config)# sme cluster c1
switch((config-sme-cl)# node 172.25.245.193
switch((config-sme-cl-node)# fabric  f1
switch((config-sme-cl-node)# interface sme 8/1 force
```

- **IOA**

  Follow these steps:

  – Scenario1: The topology has an IOA cluster with two sites, each site has at least two switches, and each switch has IOA service engines. Follow these steps:

1. Find all IOA clusters on the switch:

```
switch# show ioa cluster
```

2. Find all IOA interfaces in the cluster. Repeat this step for all IOA clusters on this switch.

```
switch# show ioa cluster <cluster-name> interface
```

From the output, find all the IOA interfaces that belong to this switch.

3. Shut all IOA interfaces on this switch:

```
switch# conf t
switch(config)# interface ioa <slot/port>
switch(config)# shutdown
```

– Scenario 2: The topology has an IOA cluster with two sites, and one or both sites have just one switch with IOA service engines. Follow these steps:

1. Find all IOA clusters on the switch.

```
switch# show ioa cluster
```

2. Find the IOA flow group and flow information for all IOA clusters

```
switch# show ioa internal info cluster <cluster name> flowgroups
```

Find the flow group name, host, and target information for each flow.

3. Remove all IOA flows.

```
switch# conf t
switch(config)# ioa cluster <cluster name>
switch(config)# flowgroup <flowgroup name>
switch(config)# no host <host pwwn> target <target pwwn>
```

General Upgrading Guidelines

Note To upgrade to NX-OS Release 4.2(7a) 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 4.2(7a).

Use the following guidelines when upgrading to Cisco MDS NX-OS Release 4.2(7a):

- Install and configure dual supervisor modules.
- Issue the **show install all impact** *upgrade-image* CLI command to determine if your upgrade will be nondisruptive.
- Be aware that you need to enable Telnet following the upgrade. See "Enabling Telnet Required After an Upgrade" section on page 22.
- 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 26.
- 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 26.
- Make note of the information concerning SANTap when performing upgrades on a Cisco MDS 9222i switch, as described in "Upgrading an MDS 9222i Switch with SANTap or Invista is Provisioned on the SSM" section on page 22.
- Be aware of the impact of an upgrade on VSAN 4079 if you are upgrading from SAN-OS Release 3.x to NX-OS 4.2(7a). See the "Upgrading Effect on VSAN 4079" section on page 23 for details.
- 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 10 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 21.

Note In addition to these guidelines, you may want to review the information in the "Limitations and Restrictions" section on page 33 prior to a software upgrade to determine if a feature may possibly behave differently following the upgrade.

Use Table 10 to determine your nondisruptive upgrade path to Cisco MDS NX-OS Release 4.2(7a), find the image release number you are currently using in the Current column of the table, and use the path recommended.

Note The software upgrade information in Table 10 applies only to Fibre Channel switching traffic. Upgrading system software disrupts IP traffic and SSM intelligent services traffic.

Table 10 Nondisruptive Upgrade Path to Cisco MDS NX-OS Release 4.2(7a)

Current Release	Nondisruptive Upgrade Path and Ordered Upgrade Steps
NX-OS:	
All 4.2(x) releases and all 4.1(x) releases	Upgrade to NX-OS Release 4.2(7a).
SAN-OS:	
Release 3.3(1c), 3.3(2), 3.3(3), 3.3(4x), and 3.3(5x).	Upgrade to NX-OS Release 4.2(7a).
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 4.2(7a).
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 4.2(7a).
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 4.2(7a).

FICON Supported Releases and Upgrade Paths

Cisco MDS NX-OS Release 4.2(7a) is not a FICON-qualified release.

Table 11 lists additional SAN-OS and NX-OS releases that support FICON. Refer to the specific release notes for FICON upgrade path information.

Table 11 FICON Supported Releases

FICON Supported Releases	
NX-OS	Release 4.2(1b)
	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 12 to determine your FICON nondisruptive upgrade path to Cisco MDS NX-OS Release 4.2(1b) 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 12 FICON Nondisruptive Upgrade Path to MDS NX-OS Release 4.2(1b)

Current Release with FICON Enabled	Upgrade Path
NX-OS 4.1(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.2(1b).
SAN-OS 3.3(1c)	You can nondisruptively upgrade directly to NX-OS Release 4.2(1b).
SAN-OS 3.2(2c)	First upgrade to SAN-OS Release 3.3(1c), and then upgrade to NX-OS Release 4.2(1b).
SAN-OS 3.0(3b)	First upgrade to SAN-OS Release 3.3(1c), and then upgrade to NX-OS Release 4.2(1b).
SAN-OS 3.0(3)	First upgrade to SAN-OS Release 3.3(1c), and then upgrade to NX-OS Release 4.2(1b).
SAN-OS 3.0(2)	First upgrade to SAN-OS Release 3.3(1c), and then upgrade to NX-OS Release 4.2(1b).
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 an MDS 9222i Switch with SANTap or Invista is Provisioned on the SSM

On an MDS 9222i switch, if SANTap or Invista is provisioned on a Storage Services Module (SSM) in slot 2, then an In Service Software Upgrade (ISSU) to NX-OS Release 4.2(1b) is not supported. The upgrade to NX-OS Release 4.2(1b) 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 4.2(1b).

Enabling Telnet Required After an Upgrade

Following an upgrade from SAN-OS 3.x to NX-OS 4.x, you need to enable the Telnet server if you require a Telnet connection. As of MDS NX-OS Release 4.1(1b), the Telnet server is disabled by default on all switches in the Cisco MDS 9000 Family. In earlier releases, the Telnet server was enabled by default.

Upgrading Effect on VSAN 4079

If you are upgrading from a SAN-OS Release 3.x to NX-OS Release 4.2(1b), and you have not created VSAN 4079, the NX-OS software will automatically create VSAN 4079 and reserve it for EVFP use.

If VSAN 4079 is reserved for EVFP use, the **switchport trunk allowed vsan** command will filter out VSAN 4079 from the allowed list, as shown in the following example:

```
switch(config-if)# switchport trunk allowed vsan 1-4080
1-4078,4080
switch(config-if)#
```

If you have created VSAN 4079, the upgrade to NX-OS Release 4.2(1b) will have no affect on VSAN 4079.

If you downgrade after NX-OS Release 4.2(1b) creates VSAN 4079 and reserves it for EVFP use, the VSAN will no longer be reserved.

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. 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 4.2(7a)

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 4.2(7a).

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 4.2(7a)" section on page 24.

- 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 NX-OS Fundamentals Configuration Guide* for information on upgrading your SSM.

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 4.2(7a) 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 Cisco MDS 9216i switch, which has a single supervisor. If you are performing an upgrade on this switch, you should follow the nondisruptive upgrade path shown in Table 10, 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 4.2(x)), 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.

Note You cannot upgrade an MDS 9120 switch or an MDS 9140 switch to Cisco NX-OS 4.x. See Table 3 for the list of switches that support Cisco NX-OS 4.x.

Resetting SNMP Notifications Following an Upgrade

The SNMP notification configuration resets to the default settings when you upgrade to Cisco NX-OS Release 4.2(1b). Use the **snmp-server enable traps** command to reenable your required SNMP notifications.

Converting Automatically Created PortChannels Before an Upgrade

Before upgrading from NX-OS Release 4.1(x) or 4.2(x) to Release 5.x, ensure that you do not have any automatically created PortChannels present in the switch configuration. Use the **port-channel persistent** command to convert an automatically created PortChannel to a persistent PortChannel. Failure to convert automatically created PortChannels prior to the upgrade can result in traffic disruption because Autocreation of PortChannels is a deprecated feature as of NX-OS Release 4.1(1b).

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:

General Downgrading Guidelines

Use the following guidelines to nondisruptively downgrade your Cisco MDS NX-OS Release 4.2(1b):

- 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 13 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 29.

Note A downgrade from NX-OS Release 4.2(7a) 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 13 to determine the nondisruptive downgrade path from Cisco NX-OS Release 4.2(1b). 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 13 applies only to Fibre Channel switching traffic. Downgrading system software disrupts IP and SSM intelligent services traffic.

Table 13 Nondisruptive Downgrade Path from NX-OS Release 4.2(7a) a

To NX-OS or SAN-OS Release	Nondisruptive Downgrade Path and Ordered Downgrade Steps
NX-OS:	
All 4.2(x) and 4.1(x) releases	1. Downgrade to NX-OS Release 4.2(x) or 4.1(x).
SAN-OS:	
All 3.3(x) releases	2. Downgrade to NX-OS Release 4.2(x) or 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 4.2(x) or 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).
All 2.0(x) releases.	1. Downgrade to NX-OS Release 4.2(x) or 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 4.2(x) or 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

Table 14 lists the downgrade paths for FICON releases. Find the image release number that you want to downgrade to in the To Release with FICON Enabled column of the table and follow the recommended downgrade path.

Table 14 FICON Downgrade Path from NX-OS Release 4.2(1b)

To Release with FICON Enabled	Downgrade Path
NX-OS 4.1(1c)	You can nondisruptively downgrade directly from NX-OS Release 4.2(1b).
SAN-OS 3.3(1c)	You can nondisruptively downgrade directly from NX-OS Release 4.2(1b).
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 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(x) to any SAN-OS 2.x release earlier than SAN-OS Release 2.1(2e). Power down the SSM and perform the downgrade. Bring up the SSM with the new bootvar set to the 2.x SSI image.
- Downgrade the SSI boot images on the SSMs on the switch to a release version supported by your Cisco SAN-OS release. Refer to the *Cisco MDS SAN-OS Release Compatibility Matrix for Storage Service Interface Images*.
- SSM intelligent services traffic switching on SSM ports is disrupted on upgrades or downgrades.
- Fibre Channel switching traffic on SSM ports is not disrupted under the following conditions:
  - All SSM applications are disabled. Use the **show ssm provisioning** command to determine if any applications are provisioned on the SSM. Use the **no ssm enable feature** configuration mode command to disable these features.

- The EPLD version on the SSM is at 0x07 or higher. Use the **show version module** *slot* **epld** command to determine your EPLD version. Refer to the *Cisco MDS 9000 Family Release Notes for Cisco MDS 9000 EPLD Images* to upgrade your EPLD image.
- Refer to the *Cisco Data Center Interoperability Support Matrix* and the "Managing Modules" chapter in the *Cisco MDS 9000 Family CLI Configuration Guide, Release 3.x*, for information on downgrading your SSM.

Downgrading an MDS 9500 Series Switch with an 8-Gbps Module Installed

If you attempt to perform a nondisruptive software downgrade from NX-OS Release 4.x to SAN-OS Release 3.x on an MDS 9500 Series switch that has an 8-Gbps module installed, the switch should display a message that the module is unsupported and stop the downgrade. Instead, the switch displays a message that the module is unsupported and proceeds with a disruptive downgrade. The following table shows the actual and expected behavior of the switch for a software downgrade.

Table 15 Downgrade Behavior on an MDS 9500 Series Switch with 8-Gbps Module Installed

Crossbar Fabric Mode	Switch Type	Software Version	Downgrade Software Version	Actual Install Behavior	Expected Install Behavior
DB mode[1]	MDS 9513 with 8-Gbps module	4.2(7a)	3.3(x)	Disruptive	Abort. Disruptive after powerdown of 8-Gbps module.
DB mode	MDS 9513 without 8-Gbps module	4.2(7a)	3.3(x)	Disruptive	Disruptive.
BM mode[2]	MDS 9513 with 8-Gbps module	4.2(7a)	3.3(x)	Abort	Abort. Nondisruptive after powerdown of 8-Gbps module.
BM mode	MDS 9513 without 8-Gbps module	4.2(7a)	3.3(x)	Nondisruptive	Nondisruptive.
BM mode	MDS 9509 or 9506 with 8-Gbps module	4.2(7a)	3.3(x)	Abort	Abort. Nondisruptive after powerdown of 8-Gbps module.
BM mode	MDS 9509 or 9506 without 8-Gbps module	4.2(7a)	3.3(x)	Nondisruptive	Nondisruptive.

1. DB mode is the fabric mode that supports Generation 3 8-Gbps modules in an MDS 9513 switch chassis.
2. BM mode is the fabric mode that does not support Generation 3 8-Gbps modules in an MDS 9513 switch chassis.

New Features in Cisco MDS NX-OS Release 4.2(7a)

Cisco MDS NX-OS Release 4.2(7a) is a maintenance release. It includes bug fixes and the following new features:

- Slow Drain Device Detection and Congestion Avoidance

  The slow drain feature provides various enhancements to detect slow drain devices that cause congestion in the network and lead to an ISL credit shortage in the traffic destined for these devices. The credit shortage affects the unrelated flows in the fabric that use the same ISL link even though destination devices do not experience slow drain. The slow drain feature also includes a congestion avoidance function.

  Note The slow drain feature is enabled by default. Before you install Cisco NX-OS Release 4.2(7a), we recommend that you read the slow drain configuration information that is available in the "Configuring Interfaces" section of the *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide.*

  The slow drain feature is not supported on the following Cisco MDS 9000 components:

  - Supervisor-1 modules
  - Generation 1switching modules
  - Cisco MDS 9216 switch, MDS 9216i switch, MDS 9120 switch, and the MDS 9140 switch

- MIB Updates

  Objects were added to the FC-FE-MIB.

  The following objects were added to FcIfErrorEntry:

  - fcIfTimeOutDiscards,
  - fcIfOutDiscards,
  - fcIfCreditLoss,
  - fcIfTxWtAvgBBCreditTransitionToZero

  Documentation for MIBs is available in the *Cisco MDS 9000 Family MIB Quick Reference.*

Licensed Cisco NX-OS Software Packages

Most Cisco MDS 9000 family software features are included in 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 are also included in this package. Refer to the Cisco MDS 9000 Mainframe 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 MDS 9000 18/4-Port Multiservice Module (MSM-18/4), 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. The Storage Media Encryption package is for use only with Cisco MDS 9000 Family switches.

Data Mobility Manager Package

The Cisco MDS 9000 Data Mobility Manager 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. The Data Mobility Manager package is for use only with Cisco MDS 9000 Family switches.

I/O Accelerator Package

The Cisco I/O Accelerator (IOA) package activates IOA on the Cisco MDS 9222i fabric switch, the Cisco MDS 9000 18/4 Multiservice Module (MSM-18/4), and on the SSN-16 module. The IOA package is licensed per service engine and is tied to the chassis. The number of licenses required is equal to the number of service engines on which the intelligent fabric application is used.The SSN-16 requires a separate license for each engine on which you want to run IOA. Each SSN-16 engine that you configure for IOA checks out a license from the pool managed at the chassis level. SSN-16 IOA licenses are available as single licenses.

XRC Acceleration License

The Cisco Extended Remote Copy (XRC) acceleration license activates FICON XRC acceleration on the Cisco MDS 9222i switch and on the MSM-18/4 in the Cisco MDS 9500 Series directors. One license per chassis is required. You must install the Mainframe Package and the SAN Extension over FCIP Package before you install the XRC acceleration license. The Mainframe Package enables the underlying FICON support, and the FCIP license or licenses enable the underlying FCIP support. XRC acceleration is not supported on the SSN-16.

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. The ability to execute the **show** command addresses the following:

- 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.
- This behavior makes Cisco MDS 9000 Series switches consistent with other Cisco products, such as Cisco Nexus 7000 Series switches, that exhibit the same behavior for those roles (when they apply to the VLAN policy).

Red Hat Enterprise Linux

The Linux kernel core dump is not supported in NX-OS Release 4.1(1b) 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(1b) 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

As of MDS NX-OS Release 4.1(1b) 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(3a).

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.

VRRP Availability

The Virtual Router Redundancy Protocol (VRRP) is not available on the Gigabit Ethernet interfaces on the MSM-18/4 module or module 1 of the MDS 9222i switch, even though it is visible on these modules. The feature is not implemented in the current release.

Using a RSA Version 1 Key for SSH Following an Upgrade

For security reasons, NX-OS Release 4.2(1b) does not support RSA version 1 keys. As a result, if you upgrade to NX-OS Release 4.2(1b) from an earlier version that did support RSA version 1 keys, and you had configured a RSA version 1 key for SSH, then you will not be able to log in through SSH following the upgrade.

If you have a RSA version 1 key configured for SSH, before upgrading to NX-OS Release 4.2(7a), follow these steps:

Step 1 Disable SSH.

Step 2 Create RSA version 2 DSA keys.

Step 3 Enable SSH.

Step 4 Delete any RSA version 1 keys on any remote SSH clients and replace the version 1 keys with the new version 2 keys from the switch.

Proceed with the upgrade to NX-OS Release 4.2(7a).

If you upgrade before disabling SSH and creating RSA version 2 keys, follow these steps:

Step 1 Open a Telnet session and log in through the console.

Step 2 Issue the **no feature ssh** command to disable SSH.

Step 3 Issue the **ssh key rsa 1024** command to create RSA version 2 keys.

Step 4 Issue the **feature ssh** command to enable SSH.

CFS Cannot Distribute All Call Home Information

In MDS NX-OS Release 4.2(1b), CFS cannot distribute the following Call Home commands that can be configured with the **destination-profile** command:

- **destination-profile** *profile_name* **transport-method**
- **destination-profile** *profile_name* **http**

The output of the **show running-config callhome** command shows configured Call Home commands:

```
switch# show running-config callhome
> version 4.1(3)
> callhome
>   email-contact abc@cisco.com <mailto:abc@cisco.com>
>   phone-contact +14087994089
>   streetaddress xyxxyx
```

```
>    distribute
>    destination-profile testProfile
>    destination-profile testProfile format XML
>    no destination-profile testProfile transport-method email
>    destination-profile testProfile transport-method http
>    destination-profile testProfile http https://xyz.abc.com
>    destination-profile testProfile alert-group all
>    transport email smtp-server 64.104.140.134 port 25 use-vrf management
>    transport email from abc@cisco.com <mailto:abc@cisco.com>
>    enable
>    commit
```

When you attempt to apply these commands in the ASCII configuration, the following commands fail:

```
>    no destination-profile testProfile transport-method email
>    destination-profile testProfile transport-method http
>    destination-profile testProfile http https://xyz.abc.com
```

To work around this issue, issue these commands after the **commit** command.

Availability of F Port Trunking and F Port Channels

Trunking F ports and trunking F port channels are not supported on the following MDS 9000 components:

- DS-C9134-K9, Cisco MDS 9134 Multilayer Fabric Switch, if NPIV is enabled and the switch is used as the NPV core switch
- DS-C9124-K9, Cisco MDS 9124 Multilayer Fabric Switch, if NPIV is enabled and the switch is used as the NPV core switch

Trunking F ports, trunking F port channels and regular F port channels are not supported on the following MDS 9000 components:

- DS-C9216i-K9, Cisco MDS 9216i Multilayer Fabric Switch
- DS-X9016, Cisco MDS 9000 2-Gbps16-Port Fibre Channel Switching Module
- DS-X9032, Cisco MDS 9000 2-Gbps 32-Port Fibre Channel Switching Module
- DS-X9032-14K9, Cisco MDS 9000 14/2-Port Multiprotocol Services Module (MPS-14/2)

For configuration information, refer to the "Configuring Trunking" section in the *Cisco MDS 9000 NX-OS Interfaces Configuration Guide*.

Reserved VSAN Range and Isolated VSAN Range Guidelines

On an NPV switch with a trunking configuration on any interface, or on a regular switch where the **feature fport_channel_trunk** command has been issued to enable the Trunking F PortChannels feature, follow these configuration guidelines for reserved VSANs and the isolated VSAN:

- If trunk mode is on for any of the interfaces or NP PortChannel is up, the reserved VSANs are 3040 to 4078, and they are not available for user configuration.
- The Exchange Virtual Fabric Protocol (EVFP) isolated VSAN is 4079, and it is not available for user configuration.
- VSAN 4079 will be impacted by an upgrade to NX-OS Release 4.1(3a), depending on whether or not VSAN 4079 was created prior to the upgrade. See the "Upgrading Effect on VSAN 4079" section on page 23 for details.

The following VSAN IDs are assigned in the Fibre Channel Framing and Signaling (FC-FS) interface standard:

VF_ID Value	Value Description
00h	Do not use as a Virtual Fabric Identifier.
001h ... EFFh	Available as a Virtual Fabric Identifier.
F00h ... FEEh	Reserved.
FEFh	Control VF-ID (see Fibre Channel Link Services (FC-LS) and Fibre Channel Switch Fabric Generation 4 (FC-SW-4) standards).
FF0h ... FFEh	Vendor specific.
FFFh	Do not use as a Virtual Fabric Identifier.
FEFh = 4079	

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.

RSPAN Traffic Not Supported on CTS Ports on 8-Gbps Switching Modules

An inter-switch link (ISL) that is enabled for Cisco TrustSec (CTS) encryption must be brought up in non-CTS mode to support remote SPAN (RSPAN) traffic on the following modules:

- DS-X9248-96K9: Cisco MDS 9000 48-Port 8-Gbps Fibre Channel Switching Module
- DS-X9224-96K9: Cisco MDS 9000 24-Port 8-Gbps Fibre Channel Switching Module
- DS-X9248-48K9: Cisco MDS 9000 4/44-Port Host-Optimized 8-Gbps Fibre Channel Switching Module

If the ISL link is brought up with CTS enabled, random packets drops of both RSPAN traffic and normal traffic will occur on the receiver port switch.

I/O Accelerator Feature Limitations

In NX-OS Release 4.2(7a), IOA does not support the following NX-OS features:

- IVR flows
- Devices with NPV and NPIV enabled
- F port trunking
- F port channeling

Support for FCIP Compression Modes

In Cisco NX-OS Release 4.2(7a), FCIP compression mode 1 and compression mode 3 are not supported on the Cisco MSM-18/4 module and on the SSN-16 module.

Saving Copies of the Running Kickstart and System Images

After you upgrade to MDS NX-OS Release 4.2(7a), you are not allowed to delete, rename, move, or overwrite the kickstart and system images that are in the current system bootvar settings on an active or standby MDS Supervisor-2 module on any Cisco MDS 9500 Series switch. This restriction does not apply to the integrated supervisor module on the MDS 9200 and MDS 9100 series switches.

Configuring Buffer Credits on a Generation 2 or Generation 3 Module

When you configure port mode to auto or E on a Generation 2 module, one of the ports will not come up for the following configuration:

- Port Mode: auto or E for all of the ports
- Rate Mode: dedicated
- Buffer Credits: default value

When you configure port mode to auto or E on a Generation 3 module, one or two of the ports will not come up for the following configuration:

- Port Mode: auto or E for the first half of the ports, the second half of the ports, or for all of the ports
- Rate Mode: dedicated
- Buffer Credits: default value

When you configure port mode to auto or E for all ports in the global buffer pool, you need to reconfigure buffer credits on one or more of the ports. The total number of buffer credits configured for all the ports in the global buffer pool should be reduced by 64.

PPRC Not Supported with FCIP Write Acceleration

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

Rule Changes Between SAN-OS Release 3.3(1c) and NX-OS Release 4.2(1a) Affect Role Behavior

The rules that can be configured for roles were modified between SAN-OS Release 3.3(1c) and NX-OS Release 4.2(1a). As a result, roles do not behave as expected following an upgrade from SAN-OS Release 3.3(1c) to NX-OS Release 4.2(1a). Manual configuration changes are required to restore the desired behavior.

Rule 4 and Rule 3: after the upgrade, **exec** and **feature** are removed. Change rule 4 and rule 3 as follows:

SAN-OS Release 3.3(1c) Rule	NX-OS Release 4.2(1a), Set the Rule to:
rule 4 permit exec feature debug	rule 4 permit debug
rule 3 permit exec feature clear	rule 3 permit clear

Rule 2: after the upgrade, **exec feature license** is obsolete.

SAN-OS Release 3.3(1c) Rule	NX-OS Release 4.2(1a) Rule
rule 2 permit exec feature license	Not available in Release 4.2(1).

Rule 9, Rule 8, and Rule 7: after the upgrade, you need to have the feature enabled to configure it. In SAN-OS Release 3.3(1c), you could configure a feature without enabling it.

SAN-OS Release 3.3(1c) Rule	NX-OS Release 4.2(1a), to Preserve the Rule:
rule 9 deny config feature telnet	Not available in Release 4.2(1) and cannot be used.
rule 8 deny config feature tacacs-server	During the upgrade, enable the feature to preserve the rule; otherwise, the rule disappears.
rule 7 deny config feature tacacs+	During the upgrade, enable the feature to preserve the rule; otherwise, the rule disappears.

Configuring a Persistent FCID in an IVR Configuration with Brocade Switches

The following information is relevant if you have a fabric that consists of Cisco MDS 9000 switches and Brocade switches, and the Cisco MDS switches are running either NX-OS Release 4.x or Release 5.x and Brocade is running FOS higher than 6.x. In an IVR configuration, when IVR NAT is enabled on a Cisco MDS 9000 switch, the device in the native VSAN should be configured with a persistent FCID. Assuming the FCID is 0xAABBCC, AA should be configured with the virtual IVR domain ID of the VSAN that contains the ISLs and BB should be configured in the following range:

- 1 through 64 if the Brocade switch is operating in native interop mode.
- 1 through 30 if the Brocade switch is operating in McData Fabric mode or McData Open Fabric Mode.

This configuration ensures that the devices connected to the Cisco MDS 9000 switch can be seen in the name server database on the Brocade switch.

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)
	4.2(5)	4.2(7a)
Severity 1		
CSCtc65441	O	R
CSCti35366	—	R
CSCto68011	—	O
Severity 2		
CSCtg48403	O	R
CSCtg92556	O	R
CSCth36768	O	R
CSCti14015	—	R
CSCty32238	O	O
Severity 3		
CSCte46238	O	R
CSCte76880	—	R
CSCte79316	O	R
CSCte93745	—	R
CSCtf09877	—	R
CSCtf44606	O	R
CSCtg11776	O	R
CSCtg20622	O	R
CSCtg20665	O	R
CSCtg29277	O	R
CSCtg39501	O	R
CSCtg61169	O	R
CSCtg66377	O	R
CSCtg79138	O	R
CSCtg81037	O	R
CSCtg86355	O	R
CSCtg90982	O	R
CSCth03492	O	R
CSCth05382	O	R

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)
	4.2(5)	4.2(7a)
CSCth21456	O	R
CSCth21997	O	R
CSCth29996	O	R
CSCth70930	O	R
CSCth88165	_	R
CSCth93476	–	O
CSCti11858	–	R
CSCti23777	–	R
CSCti33087	–	R
Severity 4		
CSCtg36047	O	R
CSCtg32977	O	R
CSCtg41212	O	R
CSCtg50316	O	R
CSCtg36399	O	R
CSCtn68418	O	O
Severity 6		
CSCtg90368	O	R
CSCtg90392	O	R
CSCth25371	O	R
CSCth34102	O	R
CSCth54422	O	R

Resolved Caveats

- CSCtc65441

  Symptom: A watchdog timeout error may cause a Cisco MDS 9124 switch to fail and reload. This symptom may occur when there is excessive traffic or errors on the mgmt0 port.

  Workaround: This issue is resolved.

- CSCti35366

  Symptom: The RSCN process on a Cisco MDS 9513 switch fails because of a heartbeat failure and the following error message is displayed.

  ```
  KERN Critical SYSTEM_MSG mts_is_q_space_available():1050:Total mtsbuf size 5027136
  for sap 21, exceeds the allowable limit of 15 percof 16777216 - kernel

  UTC RSCN Critical MTS_FAILED RSCN MTS operation failed: MTS Send notification failed::
  Device or resource busy
  ```

This symptom might occur if the there are multiple MTS requests for RCSN to process.

Workaround: This issue is resolved.

- CSCtg48403

  Symptom: FICON Tape Acceleration (FTA) may unexpectedly reload when unplugging or reinitializing a host or tape Control unit port. This symptom may be seen when a host or tape control unit port is unplugged or re-initialized after an FCIP link fails over from one higher FSPF cost FCIP link to another lower FSPF cost link. Both FCIP links must be trunking the same VSAN and FTA must be configured for that VSAN.

  Workaround: This issue is resolved.

- CSCtg92556

  Symptom: Operations involving CIM elements in the fabric profile fail.

  Workaround: This issue is resolved.

- CSCth36768

  Symptom: With XRC running, two FCIP links in a PortChannel went down. When they came back up, the PortChannel was stuck in the UP state on one side and in the initializing state on the other side. As a result, the FICON traffic did not route across the link.

  Workaround: This issue is resolved.

- CSCti14015

  Symptom: If you perform an In-Service Software Upgrade to NX-OS Release 4.2(7a), the following error message is displayed in the port monitor log.

  ```
  BB Credit not available
  ```

  This symptom might occur if the switch hardware is not configured to count the buffer credit wait time.

  Workaround: This issue is resolved.

- CSCte46238

  Symptom: The SSM module failed because of a problem with the ACL Manager.

  Workaround: This issue is resolved.

- CSCte76880

  Symptom: If the other end of the management interface on an MDS 9222i switch is configured full duplex and the MDS 9222i switch management interface is configured full duplex, the MDS 9222i switch management interface will come up in half duplex rather than full duplex. This symptom may be seen with the counterpart of the MDS 9222i switch management interface is configured in full duplex mode.

  Workaround: This issue is resolved.

- CSCte79316

  Symptom: If you enter the **show device-alias status** command while a service of device-alias is waiting for a CFS response, the output that is displayed may not be correct.

  Workaround: This issue is resolved.

- CSCte93745

  Symptom: The Com1 interface is not supported in MDS 9100 Series switches, but the related configuration and show commands are exposed.

  Workaround: This issue is resolved.

- CSCtf09877

  Symptom: You cannot create VSAN 4093 on a Cisco MDS 9134 Switch after you perform an In-Service Software Upgrade from NX-OS Release 4.2(1a) to NX-OS Release 5.0(1a).

  Workaround: This issue is resolved.

- CSCtf44606

  Symptom: On an MDS 9222i switch running Cisco NX-OS Release 4.2(3), if the mgmt0 port is configured to 100/full, it may come up as 100/half.

  Workaround: This issue is resolved.

- CSCtg11776

  Symptom: Scheduled jobs start failing approximately 24 to 48 hours after they are configured. This symptom may be seen when AAM remote authentication is configured, but does not appear in the running or saved configuration.

  Workaround: This issue is resolved.

- CSCtg20622

  Symptom: When Write Acceleration is enabled and in use with FCIP, and a third-party WAN optimization appliance takes actions on the FCIP frames, the peer FCIP switch may experience a port software failure that results in a core file.

  Workaround: This issue is resolved.

- CSCtg20665

  Symptom: Invalid TCAM threshold messages were written to syslog.

  Workaround: This issue is resolved.

- CSCtg29277

  Symptom: Cisco Discovery Protocol (CDP) cannot be enabled on a Gigabit Ethernet interface on an MDS 9000 switch running NX-OS Release 4.1(1b).

  Workaround: This issue is resolved.

- CSCtg39501

  Symptom: Upgrading the SSI image on an MSM-18/4 module in slot 2 of an MDS 9222i switch causes the Gigabit Ethernet ports in module 1 to fail with the status:

  ```
  %IMAGE_DNLD-SLOT2-2-IMG_DNLD_STARTED:  Module image download process. Please wait
  until completion...
  ```

  ```
   %IMAGE_DNLD-SLOT2-2-IMG_DNLD_COMPLETE:  Module image download process. Download
  successful.
  ```

  ```
  %PORT-5-IF_TRUNK_DOWN: %$VSAN 1%$ Interface fcip1, vsan 1 is down (Tunnel port src
  interface unbound)
  ```

  ```
  %PORT-5-IF_TRUNK_DOWN: %$VSAN 20%$ Interface fcip1, vsan 20 is down (Tunnel port src
  interface unbound)
  ```

  ```
  %PORT-5-IF_DOWN_SRC_PORT_NOT_BOUND: %$VSAN 1%$ Interface fcip1 is down (Tunnel port
  src interface unbound)
  ```

  ```
  %ETHPORT-5-IF_DOWN_UPGRADE_IN_PROGRESS: Interface GigabitEthernet1/1 is down
  (Linecard upgrade in progress)
  ```

  ```
  GigabitEthernet1/1       swFailure
  ```

  ```
  GigabitEthernet1/2       swFailure
  ```

  Workaround: This issue is resolved.

- CSCtg61169

Symptom: Users are no longer able to log in to an MDS 9000 switch via SSH. The following error is seen in the log file:

```
unable to lock password file
```

At the same time the /dev/root file system is 100 percent in use.

This symptom might occur if there are many HTTP requests that go to the built-in MDS web server. The log file of the service continues to grow until it consumes all available space in /dev/root.

Workaround: This issue is resolved.

- CSCtg66377

  Symptom: Configuration commands for pWWN based zone members fail if the WWW has digits only. The colon (:) separator is required as part of the format.

  Workaround: This issue is resolved.

- CSCtg79138

  Symptom: FCIP on a Cisco MDS 9000 Family switch fails with the following message:

  ```
  %PORT-5-IF_DOWN_PEER_RESET: %$VSAN 1%$ Interface fcip1 is down(TCP conn. reset by peer)
  ```

  This symptom may be seen when devices using iSCSI are sending in repeated TCP SYNs to the MDS 9000 switch. The iSCSI interfaces are configured and up but are not being used. The repeated TCP SYNs cause a memory leak in the IP services module.

  Workaround: This issue is resolved.

- CSCtg81037

  Symptom: The QoS Manager on the SSM failed because of a heartbeat failure. This symptom might be seen when the module reloads and then there are multiple programming requests. The QoS Manager can then get stuck in a loop.

  Workaround: This issue is resolved.

- CSCtg86355

  Symptom: Quoted strings are not permitted in the Call Home configuration for Customer ID and Site ID.

  Workaround: This issue is resolved.

- CSCtg94877

  Symptom: The remote procedure call (RPC) program that was packaged as a part of Linux exposed a vulnerability, so RPC was removed from the Linux package.

  Workaround: This issue is resolved.

- CSCtg90982

  Symptom: A failure of the ACL manager caused the SSM to reload.

  Workaround: This issue is resolved.

- CSCth03492

  Symptom: The **feature ficon** command enables FICON when the fabric-binding database does not have domain ID configured.

  Workaround: This issue is resolved.

- CSCth05382

  Symptom: NX-OS does support returning the fully qualified domain name (FQDN) from an SNMP walk in the system.sysname MIB.

Workaround: This issue is resolved.

- CSCth21456

  Symptom: The FCIP Write Acceleration feature in NX-OS Release 4.2(x) is incompatible with earlier releases. Invalid OXID messages are displayed when Write Acceleration is enabled over FCIP links when one FCIP peer switch is running NX-OS Release 4.2(x) and the other peer is running an earlier release.

  Workaround: This issue is resolved.

- CSCth21997

  Symptomless zone server process may fail under the following conditions:

  - While processing a merge request in enhanced mode, if the merge request is rejected due to an error encountered while building the full database, there is a memory leak.
  - While the zone mode gets changed from enhanced to basic, if the SFC received is rejected due to an error encountered while building full database, there is a memory leak.

  The possible scenarios that might cause an error while building the full database are as follows:

  - When a merge happens in enhanced mode, if the number of zones in the full zone database of the incoming merge request causes the total number of zones across VSANs in the receiving switch to be more than 8000.
  - When a merge happens in enhanced mode, if the full zone database received has certain attribute groups attached to its zones, and if the switch that received the merge request does not have the license for these attributes.
  - When a merge happens in enhanced mode or a change from enhanced to basic mode happens, if the incoming request contains any corrupted frames which are encountered while building the full database.

  The memory leak may be seen only if an active zoneset is present in the incoming request and is successfully parsed.

  Workaround: This issue is resolved.

- CSCth29996

  Symptom: In a two switch setup, the host and target are connected to the same switch, and use a VSAN in the second switch as a transit VSAN. After removing the transit VSAN from the IVR topology and disconnecting the ISL between the two switches, the host cannot reach the tape device.

  Workaround: This issue is resolved.

- CSCth70930

  Symptom: When multiple rules are defined for a role and one feature appears in the multiple rules for the same role, then the view of a switch chassis may appear blank in Device Manager. This symptom occurs because only the first rule for the feature is used and other rules are ignored.

  Workaround: This issue is resolved.

- CSCtg36047

  Symptom: %FCS-4-BAD_CT_FRAME syslog messages are logged. This symptom may seen when FCS does not get a response from a remote FCS within five seconds and a timeout occurs.

  Workaround: This issue is resolved.

- CSCtg32977

  Symptom: Call Home e-mail names do not support special characters.

Workaround: This issue is resolved. The following characters are now supported:
! # $ % & ' * + - / = ? ^ _ ` . { | } ~

Note If you use one of these special characters and if CFS is enabled and there is a switch that is running an image that does not support these special characters, then the configuration commit will fail.

- CSCtg41212

  Symptom: The MDS fcanalyzer cannot suppress screen output while writing a trace file with the write parameter.

  Workaround: This issue is resolved.

- CSCtg50316

  Symptom: IP name resolution does not work following an upgrade from Cisco SAN-OS Release 3.3 to Cisco NX-OS Release 4.2(5).

  Workaround: This issue is resolved.

- CSCtg36399

  Symptom: If you copy and paste the EEM SNMP policy configuration output from the **show running-config** command, it fails when applied to a device.

  Workaround: This issue is resolved.

- CSCtg90368

  Symptom: Modules failed to upgrade and they reloaded disruptively due to a lack of space to copy the new image.

  Workaround: This issue is resolved.

- CSCtg90392

  Symptom: The path rootfs or /dev/root is full on an MDS 9000 module:

  ```
  /var/log/wtmp is consuming the ramdisk space on the linecard
  ```

  Workaround: This issue is resolved.

- CSCth25371

  Symptom: The bundle indices of PortChannels are not restored properly from an old persistent storage service.

  Workaround: This issue is resolved.

- CSCth34102

  Symptom: A warning is needed when moving an application between user-defined CFS regions.

  Workaround: This issue is resolved.

- CSCth54422

  Symptom: When the number of zone members in the database approaches the 20,000 member limit, zone set activation may fail and the following error message may be displayed:

  ```
  2010 Jun 19 03:45:33 switchname %ZONE-2-ZS_CHANGE_ACTIVATION_FAILED_RESN_DOM: %$VSAN
  XXX%$ Activation failed : reason SFC retry exceeded domain XXX
  ```

  Workaround: This issue is resolved.

- CSCth88165

Symptom: If you enter the **sh logging onboard timeout0-drops** command on a Cisco MDS 9222i switch, the output that is displayed may not be correct.

Workaround: This issue is resolved.

- CSCti11858

  Symptom: The port group monitor feature on a Cisco MDS 9000 Family switch fails to generate an alarm when the configured port group bandwidth limit is exceeded.

  Workaround: This issue is resolved.

- CSCti23777

  Symptom: The port hardware fails with the following error message.

  ```
  IP_FCMAC_ERR
  ```

  Workaround: This issue is resolved.

- CSCti33087

  Symptom: The Call Home service on a Cisco MDS 9000 Family switch fails. This symptom might occur if the message level is configured before configuring the license and syslog-group-port settings.

  Workaround: This issue is resolved.

Open Caveats

- CSCto68011

  Symptom: The fcdomain service on both supervisor modules fails, which results in a reload of the device. An error message similar to the following is displayed:

  ```
  '' %SYSMGR-2-SERVICE_CRASHED: Service ''fcdomain'' (PID 4688) hasn't caught signal 11
  (core will be saved)''
  ```

  This issue affects the following products when they have SNMP configured:

  - Cisco MDS 9000 Series Multilayer switches
  - Cisco Nexus 5000 Series switches and Cisco Nexus 2000 Series, running in FC switching mode (NPV mode is not affected).

  The following products are confirmed not vulnerable:

  - Cisco Nexus 7000 Series switches
  - Cisco Nexus 4000 Series switches

  Workaround: The following workaround is available:

  Infrastructure Access Control Lists

Caution Because the feature in this vulnerability uses UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks. Infrastructure Access Control Lists (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for

this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: SNMP
!---
!---
!--- Permit SNMP traffic from trusted sources.
!---
ip access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq port snmp
ip access-list 150 permit tcp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq port snmp
!---
!--- Deny SNMP traffic from all other sources.
!---
ip access-list 150 deny udp any any eq port snmp
ip access-list 150 deny tcp any any eq port snmp
!---
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.
!---
access-list 150 permit ip any any
!--- Apply access-list to management interface
interface serial 2/0
 ip access-group 150 in
```

For more information on IP Access Control Lists see the “Configuring IPv4 and IPv6 Access Control List” section in the *Cisco MDS 9000 Family NX-OS Security Configuration Guide* at the following location:

http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/5_0/configuration/guides/sec/nxos/ipacl.html

For more information on IP Access Control Lists see the “Configuring ACLs” section in the *Cisco Nexus 5000 Series NX-OS Software Configuration Guide* at the following location:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/sec_ipacls.html

- CSCty32238

  Symptom: On certain hardware, certain Cisco MDS 9000 Series features and applications do not work. These include IVR, IOA, DMM, SME, fcflow, and SPAN.

  The following devices with hardware revision 1.5 are affected by this issue:

  - DS-X9248-96K9, 48-port 8-Gbps Fibre Channel Switching Module
  - DS-X9248-48K9, 4/44-port host-optimized 8-Gbps Fibre Channel Switching Module
  - DS-X9224-96K9, 24-port 8-Gbps Fibre Channel Switching Module

  The following devices with hardware revision 1.0 are affected by this issue:

  - DS-X9304-18K9, 18/4-Port Multiservice Module (MSM-18/4)
    For this module, the affected version is 73-14372-01A0 hardware version 1.0 (due to the new 73-number)
  - DS-C9222i-K9, Cisco MDS 9222i Multilayer Fabric Switch
    For this switch, the affected version is 73-14373-01A0 hardware version 1.0 (due to the new 73-number)

For the DS-X9248-96K9, DS-X9248-48K9 and DS-X9224-96K9 modules, the output of the **show module** command indicates whether or not the device is affected.

```
switch# sh mod 2
Mod  Ports  Module-Type                          Model              Status
---  -----  ----------------------------------- ------------------ ----------
2    24     1/2/4/8 Gbps FC Module              DS-X9224-96K9      ok

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
2    5.2(1)          <B>1.0</B>     20:41:00:0d:ec:24:f4:c0 to
20:58:00:0d:ec:24:f4:c0
```

In the preceding output, the device is hardware revision 1.0 and therefore not affected.

For the DS-X9304-18K9 and the DS-C9222i-K9, the **show module** command might indicate hardware version 1.0 due to new part numbers; however the **show sprom module** command shows the affected parts.

```
switch# sh mod 9
Mod  Ports  Module-Type                          Model              Status
---  -----  ----------------------------------- ------------------ ----------
9    22     4x1GE IPS, 18x1/2/4Gbps FC Module   DS-X9304-18K9      ok

Mod  Sw              Hw      World-Wide-Name(s) (WWN)
---  --------------  ------  --------------------------------------------------
9    5.2(1)          1.0     22:01:00:0d:ec:25:e9:80 to 22:12:00:0d:ec:25:e9:80

Mod  MAC-Address(es)                         Serial-Num
---  --------------------------------------  ----------
9    00-1a-e2-03-4c-5c to 00-1a-e2-03-4c-64  JAE1131SCBW

switch# sh sprom module 9 1 |egrep "Part|Serial"
 Serial Number   : JAE1131SCBW
 Part Number     : 73-10688-06     <-- Not 73-14372-01 so h/w ver 1.0 is OK
 Part Revision   : A0
```

Workaround: Upgrade to software release that has the fix for this issue.

- After performing a software upgrade to a Cisco NX-OS release that contains a fix for this issue, it may be necessary to enter the **shut** command followed by the **no shut** command on the affected host ports to regain connectivity.
- If you perform a nondisruptive upgrade or downgrade from a release that contains a fix to a release that does not contain the fix, you need to reload each module affected by this issue.
- If you have a Cisco MDS 9222i swtich that is affected by this issue, and you perform a nondisruptive upgrade or downgrade from a release that contains a fix to a release that does not contain the fix, you need to reload the switch.

- CSCth93476

Symptom: A SCSI flow that is configured for Fibre Channel write acceleration might disappear after a module reloads. This symptom can be seen under the following conditions:

- SCSI flows are configured and the module is reloaded.
- SCSI flows are configured and the switch is upgraded from NX-OS Release 4.2(x) to NX-OS Release 4.2(7a).

Workaround: To work around this issue, follow these steps:

1. View the currently configured SCSI flow by entering the following command:

```
switch# show scsi-flow
```

2. Delete the SCSI flow configuration from the switch. In configuration mode, enter the following command:

   ```
   switch(config)# no scsi-flow flow-id <flow-id>
   ```

   Enter this command separately for each configured SCSI flow.

3. Re-create the SCSI flows. In configuration mode, enter the following command:

```
switch(config)# scsi-flow flow-id <flow-id> initiator-vsan <initiator-vsan>
initiator-pwwn <initiator-pwwn> target-vsan <target-vasn> target-pwwn <target-pwwn>
```

4. Enable SCSI flow statistics and Fibre Channel write acceleration by entering the following commands:

```
switch(config)# scsi-flow flow-id <flow-id> statistics
switch(config)# scsi-flow flow-id <flow-id> write-acceleration>
```

- CSCtn68418

  Symptom: When you try to save a configuration, you might see the following message:

```
switch# copy run start
[########################################] 100%
Configuration update aborted: request was aborted
 %DAEMON-3-SYSTEM_MSG: ntp:can't open /mnt/pss/ntp.drift.TEMP: No space left on
device
- ntpd[xxxx]
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR
%PLATFORM-2-MEMORY_ALERT: Memory Status Alert : MINOR ALERT RECOVERED
`show system internal flash` output will display /isan as 100% full.
Mount-on                  1K-blocks      Used   Available   Use%  Filesystem
/                            204800     54624      150176     27   /dev/root
/proc                             0         0           0      0   proc
/isan                        409600    409576          24    100   none
```

  This symptom was seen because the Call Home feature had duplicate message throttling disabled and there were flapping interfaces that generated thousands of Call Home messages. These messages filled up the ISAN directory.

  Workaround: To work around this issue, enable Call Home duplicate message throttling. If you find that the /isan directory is 100 percent full, open a TAC case to get assistance with deleting the files.

Related Documentation

The documentation set for NX-OS for the Cisco MDS 9000 Family includes the following documents. To find a document online, access the following web site:

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

The documentation set for Cisco Fabric Manager appears in the *Cisco Fabric Manager Release Notes for Release 4.2(5)*, which is available from the following website:

http://www.cisco.com/en/US/products/ps10495/prod_release_notes_list.html

Release Notes

- *Cisco MDS 9000 Family Release Notes for Cisco MDS NX-OS Releases*
- *Cisco MDS 9000 Family Release Notes for 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*

Regulatory Compliance and Safety Information

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

Compatibility Information

- *Cisco Data Center Interoperability Support Matrix*
- *Cisco MDS 9000 NX-OS Hardware and Software Compatibility Information and Feature Lists*
- *Cisco MDS NX-OS Release Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family Switch-to-Switch Interoperability Configuration Guide*
- *Cisco MDS NX-OS Release Compatibility Matrix for IBM SAN Volume Controller Software for Cisco MDS 9000*
- *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9124 and Cisco MDS 9134 Multilayer Fabric Switch Quick Start Guide*

Software Installation and Upgrade

- *Cisco MDS 9000 NX-OS Release 4.1(x) and SAN-OS 3(x) Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Storage Services Interface Image Install and Upgrade Guide*
- *Cisco MDS 9000 Family Storage Services Module Software Installation and Upgrade Guide*

Cisco NX-OS

- *Cisco MDS 9000 Family NX-OS Licensing Guide*
- *Cisco MDS 9000 Family NX-OS Fundamentals Configuration Guide*
- *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*

- *Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Fabric Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Quality of Service Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Security Configuration Guide*
- *Cisco MDS 9000 Family NX-OS IP Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Intelligent Storage Services Configuration Guide*
- *Cisco MDS 9000 Family NX-OS High Availability and Redundancy Configuration Guide*
- *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*

Command-Line Interface

- *Cisco MDS 9000 Family Command Reference*

Intelligent Storage Networking Services Configuration Guides

- *Cisco MDS 9000 I/O Acceleration Configuration Guide*
- *Cisco MDS 9000 Family SANTap Deployment Guide*
- *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*
- *Cisco MDS 9000 Family Cookbook for Cisco MDS SAN-OS*

Troubleshooting and Reference

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

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.