Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 2.1(2d)

Release Date: December 19, 2005

Text Part Number: OL-7411-05 Q0

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the "Related Documentation" section on page 31.

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

Table 1 shows the on-line change history for this document.

Table 1 Online History Table

Version	Date	Description
A0	12/19/2005	Release note created
B0	12/23/2005	Added software part numbers and upgrade information
C0	12/30/2005	Added DDTS CSCei91968
D0	02/17/2006	Added DDTSs CSCsb90192, Workaround: None., CSCsc23435, CSCsc24966, CSCsc31424, CSCsc57865, CSCsc68084, CSCsc98796, CSCsc97070, CSCsd02008, and CSCsd21093 Added limitation for iSCSI proxy initiators

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

Table 1 Online History Table

Version	Date	Description
E0	05/31/2006	Added CSCeg33121, CSCsd29338, CSCeg12962, CSCeg84871, CSCeh04183, CSCeh30951, CSCeh70232, CSCei02126, CSCei10774, CSCei36082, CSCei55208, CSCei79457, CSCsc75056, CSCsc95884, CSCsd47064, CSCsd79954, CSCeg53114, CSCei57342, CSCei58652, CSCei71686, CSCei86399, CSCei91676, CSCej08751, CSCsb89732, CSCsc09732, CSCsc20106, CSCsc33788, CSCsc40012, CSCsc48919, CSCsc60283, CSCsc93936, CSCsd07246, CSCsd12831, CSCsd22920, CSCsd25790, CSCsd30165, CSCsd34882, CSCsd53429, CSCsd58774, CSCsd60578, CSCsd70927, CSCsd71701, CSCsd72822, CSCsd73494, CSCsd76429, CSCsd81725, CSCsd82449, and CSCsd94718
F0	06/06/2006	Removed DDTS CSCed16845
G0	07/10/2006	Corrected the CWDM part numbers in Table 2. Removed CSCeg33121, CSCeg12962, CSCeg84871, CSCeg90336, CSCeh04183, CSCeh30951, CSCeh52973, CSCeh70232, CSCeh93109, CSCei10774, CSCei36082, CSCei55208, CSCei55341, CSCec31365, CSCeg12383, CSCeg53114, CSCeg55238, CSCeh34828, CSCei48889, CSCei83322, CSCei91676, CSCej08751, CSCin92870, CSCin95789, CSCsd71701.
H0	08/7/2006	Added DDTS CSCse84811
I0	08/18/2006	Added DDTS CSCse89151
J0	08/22/2006	Added DDTS CSCse65400.
K0	09/5/2006	Added DDTS CSCsd78967 and CSCse88606.
L0	09/13/2006	Added DDTS CSCsf21970
M0	11/13/2006	Added DDTS CSCin95789, CSCsd81137, CSCse22145, CSCse70275, CSCse71420, CSCsf96043, CSCsg12020, and CSCsg15392.
N0	02/23/2007	Added DDTS CSCse99087, CSCsg03171, CSCsg62359, and CSCsh27840.
O0	03/26/2007	Added DDTS CSCsd41578.
P0	04/04/2007	Added the section "Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch".
Q0	08/24/2007	Added DDTS CSCsd83775.

Contents

This document includes the following sections:

Introduction

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

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

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 2.1(2d) and includes the following topics:

Components Supported

Table 2 lists the software 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	M95S1K9-2.1.2D	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S1K9-2.1.2D	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S1K9-2.1.2D	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only
License	M9500ENT1K9	Enterprise package.	MDS 9500 Series
	M9200ENT1K9	Enterprise package.	MDS 9200 Series
	M9100ENT1K9	Enterprise package.	MDS 9100 Series
	M9500FIC1K9	Mainframe package.	MDS 9500 Series
	M9200FIC1K9	Mainframe package.	MDS 9200 Series
	M9100FIC1K9	Mainframe package.	MDS 9100 Series
	M9500FMS1K9	Fabric Manager Server package.	MDS 9500 Series
	M9200FMS1K9	Fabric Manager Server package.	MDS 9200 Series
	M9100FMS1K9	Fabric Manager Server package.	MDS 9100 Series
	M9500EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9500 Series
	M9200EXT1K9	SAN Extension over IP package for IPS-8 module.	MDS 9200 Series
	M9500EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9500 Series
	M9200EXT14K9	SAN Extension over IP package for IPS-4 module.	MDS 9200 Series
	M9500EXT12K9	SAN Extension over IP package for MPS 14+2 module.	MDS 9500 Series
	M9200EXT12K9	SAN Extension over IP package for MPS 14+2 module.	MDS 9200 Series
	M9500SSE1K9	Storage Services Enabler package.	MDS 9500 Series with ASM or SSM
	M9200SSE1K9	Storage Services Enabler package.	MDS 9200 Series with ASM or SSM

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

Component	Part Number	Description	Applicable Product
Chassis	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs[1] sold separately).	MDS 9509 only
	DS-C9506	MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately).	MDS 9506 only
	DS-C9216-K9	MDS 9216 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216 only
	DS-C9216A-K9	MDS 9216A 16-port semi-modular fabric switch (includes 16 1-Gbps/2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216A only
	DS-C9216i-K9	MDS 9216i 16-port semi-modular fabric switch (includes 14 1-Gbps/2-Gbps Fibre Channel ports, 2 Gigabit Ethernet ports, power supply, and expansion slot—SFPs sold separately).	MDS 9216i only
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 host-optimized ports).	MDS 9140 only
	DS-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 only
Supervisor modules	DS-X9530-SF1-K9	MDS 9500 Supervisor/Fabric-I, module.	MDS 9500 Series only
Switching modules	DS-X9016	MDS 9000 16-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	MDS 9500 Series and 9200 Series
	DS-X9032	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel module (SFPs sold separately).	
Services modules	DS-X9308-SMIP	8-port Gigabit Ethernet IP Storage Services module.	
	DS-X9304-SMIP	4-port Gigabit Ethernet IP Storage Services module.	
	DS-X9032-SMV	32-port Fibre Channel Advanced Services Module (ASM).	
	DS-X9032-SSM	MDS 9000 32-port 1-Gbps/2-Gbps Fibre Channel Storage Services Module (SSM).	
	DS-X9560-SMC	Caching Services Module (CSM).	
	DS-X9302-14K9	14-port Fibre Channel/2-port Gigabit Ethernet Multiprotocol Services (MPS-14/2) module.	

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

Component	Part Number	Description	Applicable Product
LC-type fiber-optic SFP	DS-SFP-FC-2G-SW	2-Gbps/1-Gbps Fibre Channel — short wavelength SFP.	MDS 9000 Family
	DS-SFP-FC-2G-LW	2-Gbps/1-Gbps Fibre Channel — long wavelength SFP.	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel—short wavelength SFP.	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 1-Gbps/2-Gbps Fibre Channel — long wavelength SFP.	
	DS-SFP-GE-T	1-Gbps Ethernet SFP	
CWDM[2]	DS-CWDM-xxxx	Gigabit Ethernet and 1-Gbps/2-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm.	MDS 9000 Family
	DS-CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths.	
	DS-CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths.	
	DS-CWDMCHASSIS	Two slot chassis for CWDM add/drop multiplexer(s).	
Power supplies	DS-CAC-2500W	2500-W AC power supply.	MDS 9509 only
	DS-CDC-2500W	2500-W DC power supply.	
	DS-CAC-4000W-US	4000-W AC power supply for US (cable attached).	
	DS-CAC-4000W-INT	4000-W AC power supply international (cable attached).	
	DS-CAC-1900W	1900-W AC power supply.	MDS 9506 only
	DS-CDC-1900W	1900-W DC power supply.	
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	DS-CAC-300W	300-W[3] AC power supply.	MDS 9100 Series only
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB.	MDS 9500 Series only
Port analyzer adapter	DS-PAA-2	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	MDS 9000 Family
CD-ROM	M90FM-CD-212=	MDS 9000 Management Software and Documentation CD-ROM, spare.	MDS 9000 Family

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

Determining the Software Version

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

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

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

Upgrading Your Cisco MDS SAN-OS Software Image

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

You can nondisruptively upgrade to Cisco MDS SAN-OS Release 2.1(2d) from any SAN-OS software release beginning with Release 1.3(x). If you are running an older version of the SAN-OS, first upgrade to Release 1.3(x), and then upgrade to Release 2.1(2d).

When downgrading from Cisco MDS SAN-OS Release 2.1(2d) to Release 1.3(x), you might need to disable new features in Release 2.1(2d) for a nondisruptive downgrade. 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.

If you are upgrading from Cisco MDS SAN-OS Release 2.1(1x) to any image later than Release 2.1(2) and have IVR enabled, review CSCei88345 in the *Cisco MDS 9000 Family Release notes for Cisco MDS SAN-OS Release 2.1(2b)* for upgrade instructions.

Note Refer to the "Determining Software Compatibility" section of the *Cisco MDS 9000 Family Configuration Guide* for more details.

Performing a Disruptive Upgrade on a Single Supervisor MDS Family Switch

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

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

If you are performing an upgrade on one of those switches, you should follow the nondisruptive upgrade path listed in this section, 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, 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.

New Features in Cisco MDS SAN-OS Release 2.1(2d)

There are no new features available for this release.

Limitations and Restrictions

This section lists the limitations and restrictions for this release.

VSFN Compatibility

For the latest VSFN compatibility information, refer to the *Cisco MDS SAN-OS Release Compatibility Matrix for VERITAS Storage Foundation for Networks Software*.

iSCSI Proxy Initiators

No more than 250 iSCSI proxy initiator sessions can be active on an IPS port.

Caveats

This section lists the open and resolved caveats for this release. Use Table 3 to determine the status of a particular caveat. In the table, "O" indicates an open caveat and "R" indicates a resolved caveat.

Table 3 Open Caveats and Resolved Caveats Reference

DDTS Number	Software Release (Open or Resolved)	
	2.1(2b)	2.1(2d)
Severity 1		
CSCsd29338	O	O
Severity 2		
CSCeh73149	O	O
CSCei02126	O	O
CSCei18830	O	O
CSCei19822	O	O
CSCei53783	O	O
CSCej14208	O	R
CSCsc16506	O	O
CSCsc46451	O	R
CSCsc69478		R
CSCsc75056	O	O
CSCsc95884		O
CSCsd41578	O	O
CSCsd47064	O	O
CSCsd79954	O	O
CSCsd78967	O	O
CSCse65400		O
CSCse89151	O	O
CSCsh27840	O	O
Severity 3		
CSCef56229	O	O
CSCeg27584	O	O
CSCeg37598	O	O
CSCeh33548	O	O
CSCeh41099	O	O
CSCeh51924	O	O
CSCeh75500	O	O
CSCeh88814	O	O
CSCei32317	O	O

Table 3 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	2.1(2b)	2.1(2d)
CSCei57342	O	O
CSCei58652	O	O
CSCei71686	O	O
CSCei86399	O	O
CSCei91968	O	O
CSCin95686	O	O
CSCin95789	O	O
CSCsb89732	O	O
CSCsb90192	O	O
CSCsc09732	O	O
CSCsc16506	O	O
CSCsc18760	O	R
CSCsc20106	O	O
CSCsc23435	O	O
CSCsc24966	O	O
CSCsc28722	O	O
CSCsc31424	O	O
CSCsc33788	O	O
CSCsc40012	O	O
CSCsc40790	O	R
CSCsc48919	O	O
CSCsc53604	O	R
CSCsc57865	O	O
CSCsc58474	O	R
CSCsc60283	O	O
CSCsc68084	O	O
CSCsc72994	O	O
CSCsc93936	O	O
CSCsc97070	O	O
CSCsc98796	O	O
CSCsd02008		O
CSCsd07246	O	O
CSCsd12831	O	O
CSCsd21093		O
CSCsd22920		O

Table 3 Open Caveats and Resolved Caveats Reference (continued)

DDTS Number	Software Release (Open or Resolved)	
	2.1(2b)	2.1(2d)
CSCsd25790	O	O
CSCsd30165	O	O
CSCsd34882	O	O
CSCsd53429	O	O
CSCsd58774	O	O
CSCsd60578	O	O
CSCsd70927		O
CSCsd72822	O	O
CSCsd73494	O	O
CSCsd76429	O	O
CSCsd81137	O	O
CSCsd81725	O	O
CSCsd82449	O	O
CSCsd83775	O	O
CSCsd94718	O	O
CSCse22145		O
CSCse70275	O	O
CSCse71420	O	O
CSCse84811	O	O
CSCse88606	O	O
CSCse99087	O	O
CSCsf21970	O	O
CSCsf96043	O	O
CSCsg03171	O	O
CSCsg12020	O	O
CSCsg15392	O	O
CSCsg62359	O	O

Resolved Caveats

- CSCej14208

  Symptom: When making zone changes, even in basic mode, the zone server might complain that other sessions are active. Issuing a force commit or uncommit command fails because the command is not supported in this mode. This occurs when the zone mode changes are applied to multiple VSANs at the same time.

  Workaround: If a VSAN is stuck in this state, the only option is to disruptively suspend and not suspend the VSAN. When making mode changes, make the changes one VSAN at a time. Issue the **show zone status vsan X** command to verify the mode status of VSAN x before proceeding with the next VSAN. Another possible workaround is to look for another VSAN that has an open session and then end that session with the **no zone commit vsan xxx** command. Use the command **show zone internal vsan xxx** to check for an open session. You should then be able to issue a **no zone commit vsan yyy** to close the session opened for the original VSAN you were working with.

- CSCsc46451

  Symptom: CFS distribution may become inconsistent when a link flaps. One switch in the CFS distribution list may detect that a CFS peer has dropped from the fabric while the other CFS peers do not detect this. Subsequent CFS distributions result in incorrect updates to CFS peers.

  Workaround: Use a switch where all other switches are reachable through CFS for IVR applications and follow these steps:

  a. Issue the **show ivr vsan-topology** command and make sure that the switch auto topology is showing correct information.

  b. Issue the **ivr copy auto user** command in EXEC mode to copy the current active topology to the user-configured topology.

  Note The **ivr copy auto user** command should lock the database on all the remaining 10 IVR enabled switches.

  c. Issue the **ivr vsan-topology activate** command to activate the copied user configured topology.

  d. Type **ivr commit** to push the changes to all the remaining 10 IVR enabled switches.

  After Step d, all the IVR enabled switches should have active user-configured topology with the same entries.

  Using the switch where the problem exists with the auto topology output, follow these remaining steps:

  e. Issue the **no ivr distribute** command to isolate the switch from any remaining CFS clouds with IVR. Use the **show cfs merge status na ivr** command on all remaining switches to ensure that the current switch is removed and the output contains just the local switch.

  f. Issue the **ivr distribute** command to retrigger the CFS merge. After stabilization time, use the **show cfs merge status na ivr** command on each of the switches to verify the correct number of switches are shown.

  g. Finally, reenable auto topology by issuing the **ivr vsan-topo auto** command, followed by the **ivr commit** command. After stabilization time (around 2 to 3 minutes), you should see that auto topology is consistent on all switches.

- CSCsc69478

  Symptom: When a switchover occurs, CFS distributions initiated from other switches in the fabric might timeout and go into retry mode. This might result in the application distributions failure and consequent loss of application dependent functionality.

  Workaround: There is no workaround at the CFS level, however, applications like IVR may retry and recover.

- CSCsc18760

  Symptoms: FC ID rewrite entries may not be programmed on interfaces that are part of a PortChannel and the module containing those interfaces that are down (powered down or removed).

  This typically happens if the PortChannel is up and the module containing some of its members is down. For example, if IVR devices are communicating over a port channel. Power down a module containing a PortChannel member. Reboot the switch (without issuing the **copy running-configuration startup-configuration** command. After the reboot, the devices may not be able to communicate because FC ID rewrite entries are not programmed.

  Workaround: Issue the **copy running-configuration startup-configuration** command before you reboot when a module is powered down. Or, issue the **purge module *slot* running-config** command to purge any data related to the module that is powered down.

  Note Any other configuration related to the module will be lost.

- CSCsc40790

  Symptom: When multiple IVR-enabled switches are exporting a virtual domain into a VSAN, a duplicate LSR for the same virtual domain may be generated. As a result, the route to the virtual domain flaps periodically because of the contents of the two LSRs.

  This condition is more likely to happen when there is a larger number of switches exporting the same virtual domain into a VSAN.Before a steady state can be met, you must terminate the virtual domain exportation. This issue is seen only when the NAT mode is enabled.

  Workaround: Issue the **show fspf database** command a few times and observe the outputs to identify the domain where the route is flapping.

- CSCsc53604

  Symptom: In Cisco SAN-OS Release 2.1(2b), the power supplies on some Cisco MDS 9120 and Cisco MDS 9140 switches are flagged as unsupported. This generates a syslog message, a Call Home message, and a SNMP trap. Only certain power supplies with newer SEEPROM formats will trigger this problem.

  Workaround: None. The power supplies continue to function normally and the unsupported message can be ignored. Or, upgrade to Cisco SAN-OS Release 2.1(2d).

- CSCsc58474

  Symptom: A module might be taken offline mistakenly by a module reset, a module in a powered-down state, or a module in an unknown state. This is caused by a timing relationship issue between the supervisor and modules in the on-line health-check error handling mechanism. This occurs the following exist:

  a. You are running Cisco SAN-OS Release 2.1(2b) or earlier.

  b. You have minimally configured systems, with only a few modules present.

  Workaround: If the module is offline, remove and reinsert the module. Or, upgrade to Cisco MDS SAN-OS Release 2.1(2d).

Open Caveats

- CSCsd29338

  Symptom: The port manager might crash and a switchover might occur when FICON is configured and the MDS switch is interoperating with a CNT device. This occurs when a port is UP, a link failure happens, and the remote node ID (RNID) retry timer is activated.

  Workaround: None

- CSCeh73149

  Symptom: The VSAN suspend/resume operation facilitates network level reconfiguration and is not often used. In Cisco MDS SAN-OS Release 2.1(2), the command should not be used on a SANTap related VSAN.

  Workaround: If VSAN suspend/resume must be used, first unprovision SANTap prior to using VSAN suspend/resume.

- CSCeh92604

  Symptom: Enabling IVR-NAT on the same switch where write acceleration is enabled over a PortChannel of multiple FCIP links might result in frames from the source to the destination not transferring.

  Workaround: Do not have all of the following on the same switch:

  - IVR-NAT enabled
  - PortChannel of multiple FCIP links that can potentially carry IVR-NAT traffic
  - FCIP write acceleration enabled

  However, any two of the above three configurations are supported on the same switch.

  Note IVR in non-NAT mode can be configured with FCIP PortChannels and FCIP write acceleration on the same switch.

- CSCei02126

  Symptom: If snmpTargetAddrName and snmpTargetParamsName are set to NULL in the SNMP host/target creation, then the SNMP process crashes and may cause a switchover to the standby supervisor module.

  Workaround: When using third party tools or any other SNMP tool, set snmpTargetAddrName and snmpTargetParamsName to non-NULL values.

- CSCei18830

  Symptom: Removing zones from an active zone set may generate a system message that the zone activation has failed because of an Accept Change Authorization (ACA) failure.

  Workaround: None required. The IVR retries the activation and eventually the zone set activation succeeds.

- CSCei19822

  Symptom: An active IVR zone set on the local switch is not propagated when the commit session contains any other configuration changes.

  Workaround: For Release 2.1(2), perform an implicit commit without any changes. In the case of a merge failure and the IVR zone set is not active on remote switches but is active on a local switch, issue an implicit commit from the local switch to propagate the active zone set to the remote switches.

  For releases prior to 2.1(2), the workaround is different. Add either a dummy member to an existing zone or add a dummy zone with dummy members to the currently active IVR zone set, and then reactivate the IVR zone set. Then issue the commit command, which will propagate the active zone set to other switches.

- CSCei53783

  Symptom: An iSCSI host cannot log in to one IPS port after many supervisor module switchovers.

  Workaround: None.

- CSCsc16506

  Symptom: The following syslog message is displayed:

  ```
  Transmit Flow Control is seen for too long
  ```

  followed by link flap of the affected port. This applies only in E port mode and TE port mode of operation on Storage Services Modules (SSM) (DS-X9032-SSM) interfaces and occurs only when class-F packets are dropped due to a timeout condition. Typically, the packet timeout happens when there is serious congestion in the network, forcing the packets to stay in the switch for more than the timeout period.

  Workaround: Avoid configuring in E port mode or TE port mode on the Fibre Channel interfaces.

- CSCsc75056

  Symptom: Installing an invalid license file may cause an MDS switch to reload.

  Workaround: Recover the switch from the console port. Then request another license file from Cisco. Install the unaltered license file.

  Note Do not edit or modify an MDS license file as this makes the file invalid.

- CSCsc95884

  Symptom: The **install all** command may fail on an SSM when you downgrade from Cisco SAN-OS Release 3.0(1) to any SAN-OS 2.x release earlier than SAN-OS Release 2.1(2d) on a system with at least one SSM.

  Workaround: Power down the SSM before you downgrade the SAN-OS software. After the downgrade, power up the SSM with the new boot variable set to the appropriate Release 2.x SSI image.

- CSCsd41578

  Symptom: When a port continuously flaps, the Fibre Channel process may crash and cause a supervisor switchover.

  Workaround: Use a different port or check the host bus adapter (HBA) port.

- CSCsd47064

  Symptom: The Forwarding Information Base (FIB) process may fail if an IVR zone set push from the Fabric Manager fails because of an SNMP timeout and various switches send conflicting active IVR zone sets.

  Workaround: There are two ways to address the problem:

  - Examine the output of the **show interface mgmt 0** command to see if there is a duplex mismatch that may cause an SNMP timeout.
  - Use the **ivr distribute** command to enable Cisco Fabric Services (CFS) distribution for IVR zone or zone sets and the topology through Inter-Switch Links (ISLs).

- CSCsd79954

  Symptom: If a VSAN that is connected to a McDATA switch with Interop mode 1 participates in IVR, and the VSAN has devices that are zoned for IVR with a device in a VSAN with domain IDs not within the range 97 to 127, then there may be a loss of connectivity between the hosts and storage devices that are zoned for IVR and the devices in a normal zone.

  Workaround: Enable IVR NAT, which may be nondisruptive, or change the domain IDs of all the VSANs that need to participate with the VSAN in Interop mode 1 to the range 97 to 127.

- CSCsd78967

  Symptom: If you remove a port from a port channel or shutdown a member port of a port-channel, the ConnUnitPortStatus/State trap is not sent.

  Workaround: None.

- CSCse65400

  Symptom: If a module reloads or reinitializes on its own because of an error, and the port channel has one of its member ports on this module, in rare cases, the peer port of this member port will not forward traffic after the module comes back up.

  Workaround: Issue the **shutdown/no shutdown** command sequence on the port channel. If the problem still persists, issue the **shutdown/no shutdown** command sequence on the affected ports.

- CSCse89151

  Symptom: If you have more than 800 zones in an active zoneset for a single VSAN, your MDS 9000 switch might reload if you move from basic zoning to enhanced zoning and then read the active zoneset information.

  Workaround: Lower the number of zones in an active zoneset for a single VSAN to less than 800.

- CSCsh27840

  Symptom: While using an FCIP link for remote SPAN, it is possible that the FCIP link may flap.

  Workaround: Do not use FCIP links for Remote SPAN.

- CSCef56229

  Symptom: If an iSCSI initiator is configured differently on multiple switches, iSNS might report more targets to the initiator than the initiator can access. An iSCSI initiator would get a target error if it attempts to establish a connection.

  Workaround: None.

- CSCeg27584

  Symptom: Creating a role that has VSAN policy as “deny” requires an Enterprise License on the switch. If such a role is created on a switch that does not have the license, the switch exhibits different behavior when distribution is turned on versus when distribution is turned off.

  - If distribution is turned off, creation of the role is rejected.
  - If distribution is turned on, creation of the role succeeds but the VSAN policy continues to be "permit."

  Workaround: None.

- CSCeg37598

  Symptom: The iSNS server might crash when iSCSI is disabled and iSNS is enabled using Fabric Manager.

  Workaround: None.

- CSCeh33548

  Symptom: Tape devices can only be accessed over an FCIP tunnel in a PortChannel with write acceleration enabled if SID/DID based load-balancing is used in the VSANs.

  Workaround: Disable write acceleration or enable SID/DID based load-balancing in the VSANs if you have tape device traffic going over an FCIP tunnel in a PortChannel.

- CSCeh41099

  Symptom: Protocol and port numbers, if specified in an IP ACL assigned to an IPsec profile (crypto map), will be ignored. In an interop between Microsoft's iSCSI initiator with IPsec encryption with Cisco MDS 9000 Series switches, if IPsec is configured in the Microsoft iSCSI initiator (also the IPsec/IKE initiator), the host IPsec implementation sends the following IPsec policy:

  ```
  source IP - Host IP, dest IP - MDS IP,
  source port - any, dest port - 3260 (iSCSI), protocol - 6 (TCP).
  ```

  Upon receiving this policy, the protocol and port numbers are ignored and only the IP addresses for the IPSec policy are used. Thus, although iSCSI traffic is encrypted, non-iSCSI traffic (such as ICMP ping) sent by the Microsoft host in clear text will be dropped in the MDS port.

  Workaround: None.

- CSCeh51924

  Symptom: SNMP service might stop and restart because of a corrupted snmpTargetParamsEntry in the snmpTargetParamsTable. This corrupted entry is created when there is a null string in object snmpTargetParamsName as its index.

  Workaround: Enter a name in the snmpTargetParamsName with at least one character when creating an snmpTargetParamsEntry.

- CSCeh75500

  Symptom: A device that interfaces with SANTap may request SANTap to create a session for an ITL that was previously requested, and ITL checking is not robust.

  Workaround: Have the device validate the ITL and ensure that it does not send a request for a duplicate ITL.

- CSCeh88814

  Symptom: When SANTap is unprovisioned, the control virtual target (CVT) object is not getting cleaned up on the supervisor module.

  Workaround: To ensure that cleanup occurs, the administrator should first issue the **no santap module** ***slot-number*** **appl-vsan** ***vsan-id*** command to clean up the CVT, and then unprovision SANTap.

- CSCei32317

  Symptom: When configuring a remote SPAN (RSPAN), the Fibre Channel tunnel will not come up if it goes through more than one hop.

  Workaround: Configure the Fibre Channel tunnel explicit-path option and list every IP hop between the source and destination.

- CSCei57342

  Symptom: If a link is isolated because of a fabric-binding database mismatch, a reactivation of the corrected fabric-binding database may not initialize the ports.

  Workaround: Use the **shut** command followed by the **no shut** command to manually disable then enable the link.

- CSCei58652

  Symptom: When a reconfigure fabric (RCF) frames occurs on a VSAN, the ports may be left in a state where the fabric binding is incorrect.

  Workaround: None.

- CSCei71686

  Symptom: If iSCSI is enabled before FCIP, then the **qos** command that is configurable under a FCIP interface is not available as an option. The reverse is true as well. If FCIP is enabled first, then the **qos** command is not an option for iSCSI interfaces.

  Workaround: None.

- CSCei86399

  Symptom: A TACACS+ key that includes the less than (<) and greater than (>) characters fails when copied to an ftp server, and then copied back to the MDS switch.

  Workaround: None.

- CSCei91968

  Symptom: In a fabric with more than one switch, CFS or syslog can crash because of a PSS-FULL condition. This happens because of memory leakage in the persistent storage service (PSS) records stored by the CFS module.

  CFS internal distributions cause a PSS leakage during one of the following events:

  - An application registration and deregistration. (This is at the rate of 1 PSS record or 60 bytes per event.)
  - An ISL Link flap. (This is at the rate of two PSS records per CFS registered application. For 10 CFS registered applications, a 1000 flaps would cause a leak of about 1 MB.)

  In a stable fabric, application and regular CFS distributions do not result in PSS memory leakages.

  Workaround: None. A switchover will help in cleaning up these records but the usage of the partition remains the same (dev/shm partition). However, CFS will reuse the freed space for further PSS storage.

- CSCin95686

  Symptom: The RRD graph in the Performance Manager does not refresh on a web client opened in Mozilla or Netscape.

  Workaround: Do not use a proxy server or use the browser's Refresh button.

- CSCin95789

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

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

- CSCsb89732

  Symptom: After an upgrade from SAN-OS Release 1.3(2a) to any release lower than SAN-OS Release 3.0(1), you may see errors like the following in the syslog file:

```
2005 Sep 15 17:36:55 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:36:56 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:36:59 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
2005 Sep 15 17:37:43 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:37:44 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:37:47 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
2005 Sep 15 17:38:31 coral %SYSMGR-3-CFGWRITE_SRVFAILED: Service "fcc" failed to store
its configuration (error-id 0xFFFFFFFF).
2005 Sep 15 17:38:32 coral %SYSMGR-2-CFGWRITE_ABORTED: Configuration copy aborted.
2005 Sep 15 17:38:35 coral %SYSMGR-3-CFGWRITE_FAILED: Configuration copy failed
(error-id 0x401E0000).
```

  Workaround: After the upgrade, issue the **copy running-config startup-config** command *before* issuing the **show startup-config** command.

  If you have already encountered this issue, perform a stateful switchover, then issue the **copy running-config startup-config** command.

- CSCsb90192

  Symptom: The CFS process crashes while processing a discovery response containing null data.

  Workaround: None.

- CSCsc09732

  Symptom: If there is a port software failure at the same time as a configuration change for an FCIP interface, the configuration change can fail and subsequent configuration and **show** commands will fail for that FCIP interface.

  Workaround: None.

- CSCsc20106

  Symptom: On a Cisco MDS 9020 Fabric Switch, Fabric Manager displays a 4-Gbps Inter-Switch Link (ISL) as a 3-Gbps ISL.

  Workaround: None.

- CSCsc23435

  Symptom: System logs an error due to a xbar-ASIC interface device 6 (overflow). The error results in packet loss and, potentially, the card going into a failure state.

  The down-xbar interface ASIC (D-chip) has a mapping of hardware queues to software destination indexes (DIs).This table is initialized by hardware to map all queues to DI 0. The D-chip statically allocates packet buffers for each hardware queue during initialization. These buffers correspond to credits given to the central arbiter for the corresponding DI.

  On line cards with FCIP interfaces, the binding of DIs is performed dynamically after initialization. This means that any hardware queues that have not yet been bound to a DI will actually be giving credits to the arbiter for DI 0.

  In rare cases, the D-chip may fill up with packets causing an overflow condition and cause packets to be dropped and an error is be logged. If the condition persists for 1 second, the card goes into failure state.

  The following hardware components are affected by this error:

  - 8-port Gigabit Ethernet IP Storage Services module (DS-X9308-SMIP)
  - 4-port Gigabit Ethernet IP Storage Services module (DS-X9304-SMIP)
  - MPS-14/2 module (DS-X9302-14K9)
  - MDS 9216i switch (DS-C9216i-K9)

  Workaround: None.

- CSCsc24966

  Symptom: The following commands can sometimes hang the terminal during execution:

  - **show tech-support** commands
  - **tac-pac**

  Workaround: If you are connected through an SSH or Telnet session, shut down the session and restart a new one.

- CSCsc28722

  Symptom: Upgrading from a Cisco SAN-OS Release 1.3(x) image to a Release 2.x image can disrupt ongoing traffic because spurious RSCNs are generated during the upgrade. Hosts that have registered for the RSCN, using SCR, will receive these spurious RSCNs and hence the disruption. However, upgrading from Release 2.0(x) to Release 2.1(x) will not disrupt any traffic.

  Workaround: Suppress the RSCNs on a per interface basis during the upgrade using the **rscn suppress interface fc** *slot/port* hidden command.

  Note This configuration must be removed right after the upgrade, otherwise hosts that are registered for RSCN will never receive any RSCNs from then on.

  Note This configuration will go into the running-config. Because the running-config will be saved to the startup-config during upgrade, ensure that the configuration is removed and saved after upgrading.

Follow these steps:

1. Issue the **show rscn scr-table** command to identify the port registered for RSCN.
2. Issue the **show flogi database** command to identify the Fibre Channel interface of the port.
3. Issue the **config t** command to enter configuration mode.
4. Issue the **rscn suppress interface fc** *slot/port* hidden command to suppress RSCNs on all affected interfaces.
5. Begin the upgrade progress as you normally would.
6. Issue the **no rscn suppress interface fc** *slot/port* hidden command to allow RSCNs on all affected interfaces.
7. Issue the **exit** command to return to EXEC mode.
8. Issue the **copy running-config startup-config** command to save the running-config to the startup-config.

- CSCsc31424

  Symptom: Issuing a **no shutdown** command on an interface causes the following message to display:

  ```
  fc1/1: (error) port channel config in progress - config not allowed
  ```

  The following steps may reproduce the problem:

  1. Remove a port from a PortChannel.

     ```
     switch# config t
     switch(config)# interface fc slot/port
     switch(config-if)# no channel-group group-number
     ```

  2. Cause a system switchover.

     ```
     switch(config-if)# end
     switch# system switchover
     ```

  Note This problem does not always occur.

  Workaround:

  1. Configure a new PortChannel and add the interface.

     ```
     switch# config t
     switch(config)# interface fc slot/port
     switch(config-if)# channel-group group-number
     ```

     Where the PortChannel *group-number* does not exist.

  2. Remove the new PortChannel.

     ```
     switch(config-if)# exit
     switch(config)# no interface port-channel group-number
     ```

  3. Disable the interface.

     ```
     switch(config)# interface fc slot/port
     switch(config-if)# no shutdown
     ```

- CSCsc33788

Symptom: In rare circumstances, after you issue the **install all** command to upgrade an MDS switch, the upgrade may fail because the installer process fails. When this occurs, you may see a message like the following:

```
%CALLHOME-2-EVENT: SW_CRASH alert for service: installer
The installer failed to respond for 10 times. Exiting ...
Unable to send exit to installer. Return code -1
```

If you upgrade from 1.3(x) to 2.1 or from 2.0(x) to 2.1 and the upgrade fails, and if after the upgrade failure the supervisor modules are running the new software version, but some modules are running the older software version, then the next attempt to execute the **install all** command will trigger this problem.

You should not encounter this problem if you upgrade from 2.1 to a higher version.

Workaround: There are two ways to address this issue:

- To non-disruptively upgrade all modules that are running the older software version, issue the **install module** *module-number* **image** command.
- To disruptively upgrade the modules, issue the **reload module** *module-number* **force-dnld** command, or reinstall the module.

- CSCsc40012

  Symptom: If you use Telnet or SSH to access an MDS switch, TACACS+ authentication with the domain\username format does not work.

  Workaround: Use username@domain-name.xxx.com for TACACS+ authentication over Telnet or SSH.

- CSCsc48919

  Symptom: When a data path on a Storage Service Module (SSM) is congested, diagnostic frames that are delivered as best effort may be dropped. The Online Health Management System (OHMS) may bring down a Fibre Channel port on an SSM when congestion occurs and declare the port as failed.

  Workaround: To work around this issue, enter the following command:

  `switch(config)# **no system health module** *ssm-module-number* **loopback failure-action**`

- CSCsc57865

  Symptom: A device alias cannot be renamed using Fabric Manager. Fabric Manager is polling the description of the device and not the name or alias for the device.

  Workaround: Use the CLI to rename the device alias.

- CSCsc60283

  Symptom: In rare circumstances, an MDS 9000 Family switch may start displaying the following error messages in the log, several times per second:

  ```
  %KERN-1-SYSTEM_MSG: eepro100: wait_for_cmd_done timeout 0x801249d2 0xf0!
  ```

  When this situation occurs, Telnet access through the mgmt0 interface is impossible.

  Workaround: Access the switch through the console port.

- CSCsc68084

  Symptom: Fabric Manager generates the following exception in the Fabric Manager log when trying to activate a zone set:

  ```
  java.util.AbstractList$Itr.remove(Unknown Source)
  ```

This problem occurs under the following circumstances:

- You activate a new zone set in a VSAN using the Fabric Manager zoning dialog
- The existing active zone set is not null.
- One of the configured zones has a common zone member with one of the active zones (with the same zone name).

Workaround: None.

- CSCsc72994

  Symptom: If a user does not have a Fabric Manager Server (FMS) license, a demo or trial license counter for enhanced FMS features starts even when FMS enhanced features are not configured. You might see the following message:

  ```
  %LICMGR-3-LOG_LIC_NO_LIC: No license(s) present for feature FM_SERVER_PKG.
  Application(s) shutdown in 119 days.
  ```

  This might occur after upgrading to Cisco SAN-OS 2.1(2x). FMS status becomes InUsed although none of its features were or are actually used. This starts the 120 day evaluation period counter for FMS enhanced features.

  Note This does not have any impact on using the FM/DM for managing the switch for basic feature operations.

  Workaround: Install an FMS license.

- CSCsc93936

  Symptom: When you attempt to copy a running configuration or startup configuration to a tftp server in a single step, the operation fails.

  Workaround: Copy the configuration in two steps:

  ```
  switch# copy running-config volatile:
  switch# copy volatile: tftp:
  ```

- CSCsc97070

  Symptom: The port software might fail if more than 250 iSCSI sessions are present on an IPS port configured for proxy initiator mode.

  Workaround: Configure no more than 250 iSCSI sessions on an IPS port with proxy initiator mode configured.

- CSCsc98796

  Symptom: If tape acceleration is enabled and the FCIP link is under a heavy load, an FCIP link can flap when a status frame is returned from the tape device with a check condition. This includes expected check condition status frames such as the early warning for end-of-media frames.

  Workaround: None.

- CSCsd02008

  Symptom: During certain timing conditions, such as when a disk takes a long time to register FC4-type and FC4-feature information, IVR may not propagate the FC4-type and FC4-feature information to other VSANs and the information is missing from the name server.

  Workaround: Perform the following steps on all IVR-enabled switches before activating the IVR zone set:

  1. Use a hidden command to set an internal flag.

     ```
     switch# config t
     switch(config)# ivr knob set 0x4
     ```

  2. If the IVR zone set is already active, disable and reenable the disk interface.

     ```
     switch(config)# interface fc slot/port
     switch(config-if)# shutdown
     switch(config-if)# no shutdown
     switch(config-if)# exit
     switch(config)#
     ```

  3. Save the running configuration to the startup configuration.

     ```
     switch(config)# exit
     switch# copy running-config startup-config
     ```

  4. Verify the correct propagation of the FC4-type and FC4-feature.

     ```
     switch# show fcns database vsan vsan-id
     ```

- CSCsd07246

  Symptom: Following a successful login by a host, the **show interface** command lists an interface as “isolated due to port loopback.” In Fabric Manager, the Device Manager shows the same information about the interface.

  Workaround: None.

- CSCsd12831

  Symptom: You may be unable to add or delete a specific user name through the command-line interface, while you can add or delete other user names with no problem. The user name in question does not display in the output of a **show user-account** command; even so, it cannot be added or deleted.

  In this situation, you may see an error like the following:

  ```
  username <username>  password 0 <passwd>
  Internal CLI error: Success error in messaging
  Authentication token manipulation error
  could not change password for user:<username>
  no username <username>
  user not present
  {could not delete user <username>}
  ```

  Workaround: Open a case with Cisco TAC. There are no steps you can take to correct this problem.

- CSCsd21093

  Symptom: Sometimes, IP-ACL **show** commands may time out and appropriate error messages are seen on the CLI screen. Also, DNS queries corresponding to IP addresses configured in ACL filter specifications are sent from the switch to the DNS server whenever a **show ip access-list** command is issued.

  Workaround: No complete workaround for this problem exists. Partial workarounds include:

  - Disable DNS lookups on a switch using the no **ip domain-lookup** command in configuration mode. This command is a generic command that disables DNS lookups, which affects the IP-ACL manager and all the other IP services.Use this command with caution.
  - Selectively disable the DNS lookups before issuing IP-ACL **show** commands and turn it back on after the **show** command is completed.

- CSCsd22920

  Symptom: If the SNMP server location is configured with an empty value, then a subsequent **show running-config** command will only show one character for the SNMP server contact. If the SNMP server location is changed, then the **show running-config** command will show the number of characters in the SNMP server location plus one for the SNMP server contact.

  Workaround: The string length of the configured SNMP location should be greater than or equal to the string length of the SNMP contact.

  To make the string length for the SNMP location more or equal to the string length of the configured SNMP contact, a user can do one of the following:

  - Configure the SNMP location and SNMP contact with the same string length.
  - Add additional blank space in the SNMP location configuration.

- CSCsd25790

  Symptom: If an internal reconfiguration occurs on an MDS switch, the message that is sent to the log is the same message that is sent when external reconfigure fabric (RCF) frames are sent from the principal switch.

  Workaround: None.

- CSCsd30165

  Symptom: On an MDS 9500 Series switch running Cisco SAN-OS Release 2.1(1b), the output of the **show version** command shows the wrong value for the last reset, but this does not cause any operational problems on the switch. The output may look like the following:

```
kernel uptime is 137 days 3 hours 49 minute(s) 32 second(s)
 Last reset at -447213060 usecs after Sun Mar 18 05:59:15 2018
   Reason: Not defined
   System version:    Service: §"H
```

  Workaround: None.

- CSCsd34882

  Symptom: The SAN-OS software creates syslog message after a configuration change through the command -line interface The syslog message looks like this:

```
Vatican# 2006 Feb 8 09:00:33 Vatican %VSHD-5-VSHD_SYSLOG_CONFIG_I: Configuring console
from pts/1 (dhcp-peg3-vl30-144-254-7-182.cisco.com)
```

  Using the Fabric Manager to make the same configuration change does not result in the same syslog message:

```
Vatican# 2006 Feb 8 09:00:56 Vatican %PORT-5-IF_DOWN_ADMIN_DOWN: %$VSAN 1%$ Int erface
fc1/5 is down (Administratively down)
```

Workaround:None.

- CSCsd53429

  Symptom: After you enter the **ivr zone name** command to configure a zone, the switch displays a message that may be misleading:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name abc
fabric is locked for configuration. Please commit after configuration is done.
switch(config-ivr-zone)#
```

  The displayed message has been changed:

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr zone name abc
fabric is now locked for configuration. Please 'commit' configuration when done.
switch(config-ivr-zone)#
```

  Workaround: None.

- CSCsd58774

  Symptom: The following configuration causes excessive data collisions and reduced throughput on the management port of an MDS switch Supervisor 1 module:

  Management port configuration — Speed:100 Mbps, Duplex: Full
  Switch port configuration — Speed: 100 Mbps, Duplex: Full

  Resulting mode on management port — Speed: 100 Mbps, Duplex: Half
  Resulting mode on switch port — Speed: 100 Mbps, Duplex: Full

  Workaround: Because an MDS switch always autonegotiates the duplex mode and defaults to half duplex if the autonegotiation fails, you should configure the ports as follows:

  Management port configuration — Speed: 100 Mbps, Duplex: Auto
  Switch port configuration — Speed: Auto, Duplex: Auto

  Resulting mode on MDS — Speed: 100 Mbps, Duplex: Full
  Resulting mode on switch port — Speed: 100 Mbps, Duplex: Full

- CSCsd60578

  Symptom: A problem in Fibre Channel write acceleration on the Storage Services Module exhibited itself as a 10% to 15% performance drop once SCSI flows were established in both directions in relation to a SCSI initiator SCSI target pair.

  This issue is applicable only in configurations where a bidirectional SCSI flow is established for a given SCSI initiator SCSI target pair. In other words, for a SCSI flow in one direction, a given node in a SCSI initiator SCSI target pair acts as SCSI initiator, and for the SCSI flow in the other direction, the same node acts as a SCSI target.

  Workaround. None.

- CSCsd70927

  Symptom: Report collection in the Fabric Manager's Performance Manager stops after 48 hours. The data from the 48 hours is saved, but the connection to the database appears to be lost.

  Workaround: None.

- CSCsd72822

  Symptom: If a switch has multiple SSMs with the SCSI flow feature enabled, an SSM may fail to come up when you perform an upgrade or reload.

  Workaround: Before attempting to upgrade or reload an SSM, remove SCSI flow provisioning. Once the SSM comes back up, enable SCSI flow provisioning again.

  Follow these steps:

  1. Issue the following command to remove the provisioning:

     ```
     switch(config)# no ssm enable feature scsi-flow force module module-number
     ```

  2. Issue the following command to upgrade the SSM:

     ```
     switch# install all system bootflash:m9500-sf1ek9-mz.2.1.2d.bin kickstart
     bootflash:m9500-sf1ek9-kickstart-mz.2.1.2d.bin ssi
     bootflash:m9000-ek9-ssi-mz.2.1.2j.bin
     ```

  3. Issue the following command to reenable the SCSI flow feature when the SSM comes back online:

     ```
     switch(config)# ssm enable feature scsi-flow module module-number
     ```

  4. If the **ssm enable feature scsi-flow module** command fails, verify that the SSM is online using the following command:

     ```
     switch# show module
     ```

  5. Once the SSM is online, issue the following command:

     ```
     switch# reload module module-number
     ```

  6. Repeat Step 3 to reenable the SCSI flow feature.

Note The **force** option should be used only in Step 1.

- CSCsd73494

  Symptom: If an iSCSI port receives protocol data units (PDUs) for a write command after it has been aborted by a task management function (TMF), the buffers for these PDUs may be freed twice and this can lead to a port software failure on the iSCSI port.

  Workaround: None.

- CSCsd75284

  Symptom: When multiple tape drives are exposed to a switch over one target port, they appear as multiple LUNs behind the single target port. In this type of configuration, the FCIP link may occasionally get out of sync during error recovery, which may cause the FCIP link to flap.

  Workaround: While there is no workaround that can prevent this situation from occurring, you can disable tape acceleration for this type of configuration. The write acceleration feature continues to provide some acceleration over the FCIP link.

- CSCsd76429

  Symptom: FCIP tape acceleration causes a flap in the FCIP link when it receives duplicate CHECK CONDITION status frames from a tape device.

  Workaround: Because there is no workaround when the tape drive is functioning in this manner, we recommend that you turn off FCIP tape acceleration.

- CSCsd81137

  Symptom: Duplicate entries within an FC alias might cause an ISL isolation between your MDS 9000 switch and a Brocade switch.

  Workaround: Remove duplicate entries from the Brocade switch and the link will come up.

- CSCsd79938

  Symptom:After using the **ip access-group** command to configure an access list for the mgmt interface and saving the running configuration to the startup configuration, the **ip access-group** command is not present following a reboot of the running configuration. However, the command is in the startup configuration, and the access list is still in the configuration, but is not applied to the mgmt interface.

  Workaround: Reconfigure the command or issue a **copy startup-config running-config** command to put the command back in place.

- CSCsd81725

  Symptom: If many iSCSI initiators issue writes with immediate or unsolicited data to the iSCSI interface, the result may be a buffer congestion condition that may in turn lead to a B2B credit issue on the FC ports. This may cause these ports to flap.

  Workaround: Disable immediate and unsolicited data on the iSCSI initiators.

- CSCsd82449

  Symptom: Mode 1 FCIP compression performance degrades if the Fibre Channel frames received are 1 KB in size.

  Workaround: None.

- CSCsd83775

  Symptom: A Fibre Channel Inter-Switch Link (ISL) does not come up and it displays a fabric binding database mismatch error when fabric binding is activated. Thi s problem may be seen when a supervisor switchover occurs or is performed and this ISL comes up. The fabric binding merge activity detects an incompatible database and fails to bring up the link because an incorrect domain ID is being used by the fabric binding module. The fabric binding module on the switch where the switchover occurs would have cleared its local domain ID and be using a domain ID of zero.

  Workaround: Issue the **fcdomain restart vsan** *vsan-id* command in the VSANs of interest.

- CSCsd94718

  Symptom: In Fabric Manager, the local zone database is not synchronized.

  Workaround: None.

- CSCse22145

  Symptom: CFS coordinated distribution events are not logged in the syslogs.

  Workaround: Use the **show cfs internal session-history name** command to see the coordinated distribution events that are logged.

- CSCse70275

  Symptom: The Qlogic 2460 HBA fails to remote boot when it connects to a VT instantiated by SANTap on the SSM because the Qlogic 2460 BIOS sends a test ready unit with an invalid command reference number (CRN) and task attribute field. This same HBA can boot when SANTap and the SSM are not part of the configuration.

  Workaround:Use the Qlogic 2340 HBA.

- CSCse71420

Symptom: If you have multiple switches with IVR, and there is a mismatch of IVR VSAN topology and IVR zones which were corrected later, you might get an error message in the logs %FSPF-3-IPC_PROC_ERR: Error in processing IPC message : Opcode = 68, Error code = 401a0013

Workaround: None. This issue is resolved.

- CSCse84811

  Symptom: In a system with autocreate PortChannel configured, if there are multiple link flaps or configuration changes on a PortChannel, the PortChannel Manager process memory might run out causing the PortChannel Manager process to crash.

  Workaround: Issue the **write erase** command and reload the switch.

- CSCse88606

  Symptom: Setting a value higher than 4 for the maximum number of times a packet is retransmitted before TCP closes the connection might product unexpected results. This would occur during a link FCIP tunnel recovery after a short downtime.

  Workaround: Configure the TCP maximum retransmissions to values between 1 and 4 only.

- CSCse99087

  Symptom: A user called snmp-user can successfully log into an MDS switch through the CLI, but cannot log in through Fabric Manager or Device Manager. The login attempt fails with this error: `SNMP: Unknown username`

  Workaround: None.

- CSCsf21970

  Symptom: If you issue immediate, back-to-back commands to delete and then create FCIP interfaces, the internal port service might crash.

  Workaround: Wait 5 seconds between the delete and the following create command for a given FCIP interface.

- CSCsf96043

  Symptom:No alerts are issued for FCS errors on the sup-fc0 port even though it might affect Fibre Channel communication.

  Workaround: None.

- CSCsg03171

  Symptom: The dynamic port VSAN membership (DPVM) failed after the number of F ports exceeded 64 and a port flap occurred.

  Workaround: Keep the number of F ports in a switch below 64.

- CSCsg12020

  Symptom: If your switch is up for a long period of time, such as more than 100 days, zone set activation in Fabric Manager might not reflect the latest results and active-local differences may still be shown.

  Workaround: Close and reopen Fabric Manager with the "Accelerate Discovery" option unchecked. This reflects the latest change, but might need to be done after every change.

- CSCsg15392

  Symptom: If a Generation 1 module has any port that is administratively up, but operationally down when you upgrade from SAN-OS Release 2.x to either Release 3.0(1) or Release 3.0(2x), you might experience traffic disruption on that module.

Workaround: Use the **shutdown** command to shut all the ports operationally down and administratively up on all the Generation 1 modules before upgrading from SAN-OS Release 2.x to Release SAN-OS 3.0(x) or Release 3.0(2x). After the upgrade is complete, the ports can be brought to an administratively up state using the **no shutdown** command.

- CSCsg62359

  Symptom: If a user attempts to log in using TACACS+ authentication to an MDS switch or an SSH server configured on the switch, the login might fail if password-authentication is the first login method the user tries.

  Workaround: Use the keyboard-interactive method as the first login method for SSH.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents. To find a document online, use the Cisco MDS SAN-OS Documentation Locator at: http://www.cisco.com/en/US/products/ps5989/products_documentation_roadmap09186a00804500c1.html.

For information on IBM TotalStorage SAN Volume Controller Storage Software for the Cisco MDS 9000 Family, refer to the IBM TotalStorage Support website: http://www.ibm.com/storage/support/2062-2300/

Release Notes

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

Compatibility Information

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

Regulatory Compliance and Safety Information

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

Hardware Installation

- *Cisco MDS 9500 Series Hardware Installation Guide*
- *Cisco MDS 9200 Series Hardware Installation Guide*
- *Cisco MDS 9216 Switch Hardware Installation Guide*
- *Cisco MDS 9100 Series Hardware Installation Guide*
- *Cisco MDS 9020 Fabric Switch Hardware Installation Guide*

Cisco Fabric Manager

- *Cisco MDS 9000 Family Fabric Manager Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Fabric Manager Online Help*

Command-Line Interface

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

Troubleshooting and Reference

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

Installation and Configuration Note

- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family Port Analyzer Adapter Installation and Configuration Note*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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