Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 1.2(1b)

Release Date: November 6, 2003

Text Part Number: OL-4391-03, Rev. G0

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 17.

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 Note*: 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 On-Line Change History

Revision	Date	Description
A0	9/2/2004	Added DDTS CSCed64425.
B0	01/21/2005	Modified DDTS CSCee06496.
C0	2/22/2005	Added DDTS CSCee89946.
D0	3/24/2005	Added workaround information to all resolved caveats. Added DDTS CSCdz12179, CSCeb71406, CSCec03539,CSCec06947, CSCec08028, CSCec15273, CSCec17467, CSCec23079, CSCec23320, CSCec24378, CSCec25886, CSCec27835, CSCec29150, CSCec30443, CSCec31567, CSCec34016, CSCec38706, CSCec52509, CSCec53210, CSCed32729, CSCed58155, CSCed65607, CSCed75825, CSCee01143, CSCee43249, CSCeg61535, CSCeh21199. Modified DDTS CSCed21583, CSCed21595, CSCeb86793. Removed DDTS CSCeb83751. Resolved in a previous release.

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

Table 1 On-Line Change History (continued)

Revision	Date	Description
E0	06/23/2005	Added DDTS CSCei25319
F0	05/02/02006	Added DDTS CSCeg84871
G0	02/26/2007	Added DDTS CSCsh27840.

Contents

This document includes the following section:

Introduction

The Cisco MDS 9000 Family of multilayer directors and fabric switches offer intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. They combine robust and flexible hardware architecture with multiple layers of network and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9000 Family 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 1.2(1b) and includes the following topics:

Hardware Supported

Table 2 lists the hardware components supported on the Cisco MDS 9000 Family and the minimum software version required. See the "Determining the Software Version" section on page 4.

Table 2 Cisco MDS 9000 Family Supported Hardware Modules and Minimum Software Requirements

Component	Part Number	Description	Applicable Products
Software	M95S1K9-1.2.1	MDS 9500 Series supervisor/fabric-I, enterprise software	MDS 9500 Series only
	M92S1K9-1.2.1	MDS 9216 enterprise software	MDS 9216 only
	M91S1K9-1.2.1	MDS 9100 Series enterprise software	MDS 9100 Series only
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 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 sixteen 1 / 2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately)	MDS 9216 only
	DS-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 oversubscribed ports)	MDS 9120 only
	DS-C9140-K9	MDS 9140 fixed configuration (non-modular) fabric switch (includes 8 full rate ports and 32 oversubscribed ports)	MDS 9140 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 2/1-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9216
	DS-X9032	MDS 9000 32-port 2/1-Gbps Fibre Channel module (SFPs sold separately)	
Services modules	DS-X9308-SMIP	An eight-port (8) Gigabit Ethernet IP storage services module.	
LC-type fiber-optic SFP[1]	DS-SFP-FC-2G-SW	2/1-Gbps Fibre Channel — short wave SFP	MDS 9000 Family
	DS-SFP-FC-2G-LW	2/1-Gbps Fibre Channel — long wave SFP	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 2/1-Gbps Fibre Channel—short wave SFP	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 2/1-Gbps Fibre Channel — long wave SFP	

Table 2 Cisco MDS 9000 Family Supported Hardware Modules and Minimum Software Requirements (continued)

Component	Part Number	Description	Applicable Products
CWDM[2]	CWDM-SFP-xxxx-2G	Gigabit Ethernet and 2/1-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9000 Family
	CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths	
	CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths	
	CWDM-CHASSIS-2	Two slot chassis for CWDM add/drop multiplexer(s)	
Power supplies	DS-CAC-300W	300W AC power supply	MDS 9100 Series only
	DS-CAC-845W	845W[3] AC power supply	MDS 9216 only
	DS-CAC-2500W	2500W AC power supply	MDS 9509 only
	DS-CDC-2500W	2500W DC power supply	
	DS-CAC-4000W-US	4000W AC power supply for US (cable attached)	
	DS-CAC-4000W-INT	4000W AC power supply international (cable attached)	
	DS-CAC-1900W	1900W AC power supply	MDS 9506 only
	DS-CDC-1900W	1900W DC power supply	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB	MDS 9500 Series only
Port analyzer adapter	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

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

Determining the Software Version

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

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

Image Upgrade

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 (or downgrade from) Release 1.2(1b) using any Cisco MDS SAN-OS software release other than Release 1.0(2a).

New Features in Release 1.2(1b)

SAN-OS Release 1.2(1b) is a patch release for switches in the Cisco MDS 9000 Family. See the "Caveats" section on page 6 for details on closed and outstanding caveats and limitations.

Note The *Release Notes* are specific to this maintenance release. For the rest of the 1.2(1b) documentation, refer to the Release 1.2(1a) document set (see the "Related Documentation" section on page 17).

Limitations

To perform an upgrade from Release 1.2(1a) to Release 1.2(1b), or from 1.2(1b) to 1.2(1a), follow these steps:

Step 1 Log into the switch through the console port, an SSH session, or a Telnet session.

Step 2 Change to configuration mode.

```
switch# config terminal
```

Step 3 Specify the kickstart image to be used for the reboot.

```
switch(config)# boot kickstart bootflash:kickstart-image
```

Note You can only specify one image for the KICKSTART variable.

Step 4 Specify the system image.

```
switch(config)# boot system bootflash:system-image
```

Step 5 Save the new variable configuration so the new image is used the next time you log into the switch.

```
switch# copy running-config startup-config
```

Step 6 Reboot the switch.

```
switch# reload
This command will reboot the system. (y/n)? y
```

The **reload** command reboots the system and updates the variable in one or both supervisor modules automatically.

Step 7 Use the **show version** command to verify the updated image on the supervisor module.

```
switch# show version
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2003 by Cisco Systems, Inc. All rights reserved.
The copyright for certain works contained herein are owned by
Andiamo Systems, Inc. and/or other third parties and are used and
distributed under license.

Software
  BIOS:      version 1.0.8
  loader:    version 1.1(2)
  kickstart: version 1.2(1a) [build 1.2(1b)] <-----------------current running version
  system:    version 1.2(1a) [build 1.2(1b)] <-----------------current running version
```

Step 8 Issue the **show module** command to verify that the supervisor module in Slot 6 is running the new image.

Note The next time you reboot the switch, the saved image is used. If you do not save the configuration, the previously saved startup configuration image is used.

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, "R" indicates a resolved caveat, and "O" indicates an open caveat.

Table 3 Release Caveats and Caveats Corrected Reference

	Software Release (Resolved or Open)	
DDTS Number	**1.2(1a)**	**1.2(1b)**
Severity 1		
CSCeb83751	R	R
Severity 2		
CSCeb71406	O	O
CSCec15273	O	O
CSCec24378	O	O
CSCec27835	O	O
CSCec30443	O	O
CSCec38706	O	O
CSCec52509	O	O
CSCec53210	O	O
CSCed21583	O	O
CSCed21595		O
CSCed65607	O	O
CSCed75825	O	O
CSCee01143	O	O
CSCee06496	O	O
CSCee43249	O	O
CSCeg84871	O	O
CSCei25319	O	O
CSCsh27840	O	O
Severity 3		
CSCdz12179	O	O
CSCdz43707	O	O

Table 3 Release Caveats and Caveats Corrected Reference (continued)

	Software Release (Resolved or Open)	
DDTS Number	1.2(1a)	1.2(1b)
CSCea45726	O	O
CSCea82028	O	O
CSCeb19588	O	O
CSCeb34865	O	O
CSCeb75360	O	O
CSCeb83984	O	O
CSCeb84217	O	O
CSCeb86793	O	R
CSCec00031	O	O
CSCec03298	O	O
CSCec03539	O	O
CSCec06947	O	O
CSCec08028	O	O
CSCec17467	O	R
CSCec23079	O	R
CSCec23320	O	R
CSCec25886	O	R
CSCec29150	O	O
CSCec31567	O	R
CSCec34016	O	R
CSCed32729	O	O
CSCed58155	O	O
CSCed64425	O	O
CSCee89946	O	O
CSCeg61535	O	O
CSCeh21199	O	O

Resolved Caveats

- CSCeb83751

  Symptom: A Cisco MDS 9500 director, with 16-port modules currently running version 1.1(2), 1.1(3), or 1.2(1A), that was non-disruptively upgraded from version 1.0(x), 1.1(1), or 1.1(1A) and then encountered a link reinitialization on one of the 16 ports can cause the system to get into an unpredictable state and may require a switch reset to recover.

  Workaround: To prevent this unpredictable state, proactively reset the 16 port line-card after the upgrade. The following command can be used for this purpose:

  ```
  reload module <module-num>
  ```

To proactivly power-cycle the affected switching module(s) after completing the upgrade procedure specified in the *Cisco MDS 9000 Family Configuration Guide*, follow these steps:

1. Identify the Fibre Channel modules that need to be reset in the MDS switch using the **show module** command.

```
switch# show module
Mod Ports Module-Type Model Status
--- ----- ------------------ ----- ------------
4 16 1/2 Gbps FC Module DS-X9016 ok
5 0 Supervisor/Fabric-1 DS-X9530-SF1-K9 active *
...
```

In this example, only module 4 needs to be reset.

2. Issue the **reload module** command to reset the identified module. This command power cycles the selected module.

```
switch# reload module number
```

Where number indicates the slot in which the identified module resides. For example:

```
switch# reload module 4
```

3. Verify the Fibre Channel module that was reset in the MDS switch using the **show module** command. The same command issued within a few seconds of each other displays the varying states of the reloaded Fibre Channel module in this recently upgrade Cisco MDS 9500 Series Director.

```
switch# show module
Mod Ports Module-Type Model Status
--- ----- ------------------ ----- ------------
4 16 1/2 Gbps FC Module DS-X9016 pwr-cycled
5 0 Supervisor/Fabric-1 DS-X9530-SF1-K9 active *
...

switch# show module
Mod Ports Module-Type Model Status
--- ----- ------------------ ----- ------------
4 16 1/2 Gbps FC Module DS-X9016 powered-up
5 0 Supervisor/Fabric-1 DS-X9530-SF1-K9 active *
...

switch# show module
Mod Ports Module-Type Model Status
--- ----- ------------------ ----- ------------
4 16 1/2 Gbps FC Module DS-X9016 ok
5 0 Supervisor/Fabric-1 DS-X9530-SF1-K9 active *
...
```

- CSCeb86793

  Symptom: If SNMP role-based users modify their own roles using the Device Manager, then the rules for those role are removed and those users will not be able to connect to the switch using SNMP.

  Workaround: None.

- CSCec17467

  Symptom: After creating a read-only zone using Fabric Manager version 1.2(1), if you select the zone in the left hand pane (in the tree), the Members tab in the top pane may be empty.

  Workaround: None. Upgrade to Cisco MDS SAN-OS Release 1.2(2a).

- CSCec23079

  Symptom: Incorrect, large values are returned for SysUptime queries by the MDS SNMP agent.

  Workaround: None. Upgrade to Cisco MDS SAN-OS Release 1.2(2a).

- CSCec23320

  Symptom: Removing enclosures using the Fabric Manager removes member ports from fabric map.

  Workaround: None. Upgrade to Cisco MDS SAN-OS Release 1.2(2a).

- CSCec25886

  Symptom: While upgrading from 1.0(x) to 1.2(1a) space is not created in forwarding tables for new MPLS segments using remote span. This causes RSPAN to fail.

  Workaround: None. Upgrade to Cisco MDS SAN-OS Release 1.2(2a).

- CSCec31567

  Symptom: When a VSAN with the **interop 2** option in a Cisco MDS 9000 Family switch is configured to interoperate with a Brocade switch running in Native mode, the Cisco MDS switch permits the use of $ and - characters in zone set, zone, and alias names. The Brocade switch rejects zone updates containing objects with these special characters, and in some situations may isolate the ISL and segment the fabric.

  Workaround: When administering zoning from an MDS switch, be sure that the zone set, zone, and alias names do not include “$” and “-” characters. The underscore character is permitted.

- CSCec34016

  Symptom: When two TE ports are configured as a part of port channels, the transition ports intermittently show up as invalid ports in the Fabric Manager. They later merge to come up as PortChannel.

  Workaround: None. Upgrade to Cisco MDS SAN-OS Release 1.2(2a).

Open Caveats

- CSCeb71406

  Symptom: When more than one change is detected within a 50 msec window in the membership of the egress port of an existing route, the Forwarding Information Base (FIB) properly pauses the Virtual Output Queues (VOQs) of the newly added egress ports. When the pause timer expires, instead of resuming the VOQs of the paused ports related to this timer, the FIB resumes the VOQs of the paused ports related to the last timer started.

  Workaround: None.

- CSCec15273

  Symptom: When node positions are fixed on the Fabric Manager topology map, switches may disappear from the topology map if links to devices are physically moved between different switch ports.

  Workaround: None.

- CSCec24378

  Symptom: The **show version** command output may create a core file when a image is downgraded. This does not impact system behavior.

  Workaround: None.

- CSCec27835

  Symptom: When the port security or the fabric binding features are enabled in switches in the Cisco MDS 9000 Family, you cannot add members to Gigabit Ethernet PortChannels.

  Workaround: None.

- CSCec30443

  Symptom: The iSCSI host cannot open an iSCSI session to the IPS module when the TCP selective acknowledgement (SACK) option is enabled. The Cisco iSCSI initiator for Windows 2000, version 3.1.2, is not able to initiate an iSCSI session to an IPS-8 in an MDS 9509 running SAN-OS 1.2(1a).

  Workaround: Downgrade to SAN-OS 1.1.

- CSCec38706

  Symptom: When you issue a REPORT_LUNS inquiry to a XIOtech storage target, an unusual check condition with 0x062900 (Unit Attention due to power down/up, bus reset...) is returned.

  Workaround: None.

- CSCec52509

  Symptom: If a Fabric Manager client has two NIC cards and launches the Fabric Manager, the resulting dialog box allows you to choose between the two NICs. SNMP times out, regardless of which NIC is selected.

  Workaround: Use Device Manager.

- CSCec53210

  Symptom: After upgrading to Release 1.2(2), a rare combination of removing a switching (or services) module and deleting a VSAN may cause the standby supervisor module to remain in the down state.

  Workaround: Follow these steps to reload the switch, or upgrade to Cisco MDS SAN-OS Release 1.2(2a).

  1. Issue the command:

  ```
  copy startup-config bootflash:saved-config
  ```

  2. Issue the command:

  ```
  write erase
  ```

  3. Issue the command:

  ```
  copy bootflash:saved-config startup-config
  ```

  4. Reload. Standby should come up properly.

- CSCed21583

  Symptom: Upgrading from Release 1.2(1a) to 1.2(1b), or downgrading from 1.2(1b) to 1.2(1a) is disruptive. Using the installer does not upgrade line cards and switchover because the SRG is same.

  Workaround: None. Do not use “install all” to upgrade from 1.2(1a) to 1.2(1b) or to downgrade from 1.2(1b) to 1.2(1a). The recommended procedure is to copy the images onto the supervisors, set the boot variables and then reboot the system.

- CSCed21595

  Symptom: The **show version** command output for Release 1.2(1b) displays the following software image information.

  ```
  Software
    BIOS:      version 1.0.8
    loader:    version 1.1(2)
    kickstart: version 1.2(1a) [build 1.2(1b)] <-----------------current running version
    system:    version 1.2(1a) [build 1.2(1b)] <-----------------current running version
  ```

  Workaround: None.

- CSCed65607

  Symptom: A vulnerability in the Transmission Control Protocol (TCP) specification (RFC 793) was discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the attacked protocol, a successful attack may have additional consequences beyond terminated connection. This attack vector is only applicable to those sessions terminating in a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality. All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at the following website, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

  Workaround: Depending on the application, the connection may get automatically reestablished. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session).

- CSCed75825

  Symptom: If a spare supervisor module has the local boot variables pointing to Release 1.0(1) or 1.0(2) images, inserting that spare supervisor module into a functioning switch will cause the active supervisor module to fail. This issue exists in all releases up to and including Release 1.3(3c).

  Workaround: If the active supervisor runs any of the affected releases, check the version of the spare supervisor module before inserting it, or issue the **reload module** *slot-number* **force-dnld** command immediately after the insertion. The *slot-number* is the number of the slot in which the spare module is inserted.

- CSCee01143

  Symptom: When trying to access Fabric or Device Manager using SNMPv3, the user is unable to access the switch and is prompted with the error message "notintimewindow".

  Workaround: Set the clock on the switch to the highest, and then to the lowest. From there, set it back to the regular time.

- CSCee06496

  Symptom: If you are running Cisco MDS SAN-OS releases 1.1(3), 1.2(1a), 1.2(1b), 1.2(2a), 1.3(1), 1.3(2a), 1.3(3), or 1.3(3c), the following sequence of operations might lead to the failure of one or both supervisor modules simultaneously:

  a. Removing an IPS-8 module from the switch.
  b. Inserting a different type of module in the same slot.
  c. Configuring the new module.
  d. Issuing the **copy running-config startup-config** command.

  Removing the IPS-8 module at any time and replacing with another IPS-8 module does not cause this problem.

  Workaround: Before replacing an IPS-8 module with a different type of module in the same slot, upgrade to Cisco MDS SAN-OS Release 1.3(4a).

- CSCee43249

  Symptom: If a malfunctioning device does not swap the source and destination FCIDs, a PLOGI frame sent by this device can cause high CPU utilization. These PLOGI frame errors are reported by the zone server.

  Workaround: None.

- CSCeg84871

  Symptom: When an iSCSI initiator logs in to a Gigabit Ethernet port number 1 on an IPS module in slot 1, the switch sends a login response with the value of the Target Session Identifying Handle (TSIH) field set to zero (0), which is an iSCSI protocol violation. This situation can also occur when an iSCSI initiator logs in to Ethernet PortChannel number 1. The Qlogic iSCSI initiator may verify the TSIH value and reject it.

  Workaround: None.

- CSCei25319

  Sympton: An error message in the log file occurs because the platform manager component passes the wrong parameter while responding to a SNMP query. In some cases, this results in the query not being responded to.

  Workaround: Perform a refresh on Device Manager to clear the problem.

- 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.CSCsh27840

- CSCdz12179

  Symptom: When the Fabric Manager or Device Manager communicates with the Cisco MDS switch through Virtual Private Network (VPN) or any Network Address Translation (NAT) scheme, a generic error message occurs while adding duplicate zone members from a VPN connection.

  Workaround: None. If an error occurs while running through VPN/NAT, all errors will show up as generic errors without a detailed message describing the error.

- CSCdz43707

  Symptom: The Fabric Manager or Device Manager reports an error for all operations if the switch is multihomed (both IPFC-based in-band management and the out-of-band management interface are up) and the Fabric or Device Manager was started using the IPFC address. Typically, you will see a `notInTime window` error in the Device Manager and all SNMP set operations fail.

  Workaround: If the switch is multihomed, then start the Fabric or Device Manager on the switch using the out-of-band management interface IP address.

- CSCea45726

  Symptom: The Device Manager shows a port in the down state (red square) when the operational status of the port is up. This rare occurrence is due to the failure cause of the port not being empty (for example, the failure case reflects the `initializing` state).

  Workaround: None.

- CSCea82028

  Symptom: When a switch is upgraded while the Device Manager for that switch is open, a Java error of class cast exception occurs. When this error occurs, some Device Manager menu items are unusable while other menu items remain in this error state.

  Workaround: Close the Device Manager and reopen it.

- CSCeb19588

  Symptom: Sometimes, the **zone merge import** command results in isolation.

  Workaround: Reissue the command to resolve the isolation problem.

- CSCeb34865

  Symptom: The following error message is issued when you try configuring switch drop latency:

  ```
  changing this parameter is not allowed could not update the value
  ```

  Workaround: None. Switch drop latency is not configurable in this release of the software.

- CSCeb75360

  Symptom: When issuing a command that shows PortChannels (such as **show interface port-channel** or **show port-channel summary**), EtherChannel interfaces are also displayed in the VSAN membership database. This does not cause any performance issues.

  Workaround: None.

- CSCeb83984

  Symptom: When downgrading a Cisco MDS 9000 Family switch to an older release version which does not contain the LUN zoning feature, for example, Release 1.1(x), the configuration is not erased completely.

  Workaround: Delete the LUN zoning configuration before downgrading the switch.

- CSCeb84217

  Symptom: When running the **install module loader** command, you must wait for this command to finish before issuing the **reload module** command or the system will hang.

  Workaround: None.

- CSCec00031

  Symptom: While configuring an “ip access-list” and a switchover occurs for whatever reason, the standby may only have partial ip access-list information. This results in an inconsistency in applying the ip access-list policy after switchover. If this occurs, remove that recently configured ip access-list and configure it again.

  Workaround: None.

- CSCec03298

  Symptom: For iSCSI hosts connected to Cisco MDS switches, XIOtech storage devices may not be visible as iSCSI targets.

  Workaround: None.

- CSCec03539

  Symptom: Using the Fabric Manager, you may set a NULL server address for the syslog and RADIUS servers.

  Workaround: None. You must set the correct address.

- CSCec06947

  Symptom: A FC-tunnel interface is not completely displayed when configured as a SPAN destination using the Fabric Manager application.

  Workaround: None.

- CSCec08028

Symptom: The Fabric Manager provides an option to choose a NIC from within a multi-NIC system, but the Device Manager does not provide this option. If the Device Manager is opened from the Fabric Manager, this feature still works. If the Device Manager is opened from a desktop, a timeout error occurs.

Workaround: Start the Device Manager from the command line, using the option **-Dmds.nmsAddress=XX** to set a preferred address.

- CSCec29150

  Symptom: Activating a zone using the Fabric Manager fails when the interop mode is enabled, but works from the CLI.

  Workaround: None. Upgrade to Cisco MDS SAN-OS Release 1.2(2a).

- CSCed32729

  Symptom: When altering an Fx-port state using SNMP, the following error is reported:

  ```
  snmpset: Agent reported error with variable #1.
  .iso.org.dod.internet.mgmt.mib-2.75.1.2.2.1.1.22.0:  SNMP: A general
  failure occurred on the agent.
  ```

  Workaround: None.

- CSCed58155

  Symptom: The Fabric Manager (FM) cannot correlate an iSCSI host with two NIC cards when the iSCSI initiator is identified by the IP address (either from a matching static **iscsi initiator ip-address** command or from an iSCSI interface **switchport initiator id ip-address** command for dynamic initiators). This is a result of the switch putting IP address in the symbolic-node-name field in the FCNS entry for that initiator. This was done to allow zoning based on IP address in ISAN software Release 1.1(x) and 1.2(x) where zone membership for iSCSI initiator can only be based on symbolic-node-name value.

  Workaround: To allow FM to show the above-mentioned host properly, the switch will instead fill the FCNS entry's symbolic-node-name field with the actual iSCSI initiator node name (i.e. its IQN name).

  This impacts for users who configure zoning based on iSCSI initiator's IP address via the symbolic node name field, e.g.

  ```
  zone name a vsan 1
  member symbolic-nodename 10.2.2.112
  ```

  Change the above configuration to the following for this configuration to continue working after upgrading to Release 1.3(4a).

  ```
  zone name a vsan 1
  member ip-address 10.2.2.112
  ```

- CSCed64425

  Symptom: You can TFTP to a Cisco MDS switch through the management interface from any TFTP client. In SAN-OS Releases 1.3(4a), 1.3(4b) and 1.3(5), a default IP access control list (ACL) rule is added to block frames for ports like TFTP, SUNRP and BOOTP.

  Workaround: For SAN-OS Releases 1.2(1a), 1.2(1b), 1.2(2a), 1.3(1), 1.3(2a), 1.3(3), and 1.3(3c), manually create the drop rule by issuing the following commands in succession:

  ```
  switch(config)# ip access-list abc deny udp any any eq port 69
  switch(config)# ip access-list abc permit ip any any
  switch(config)# interface mgmt 0
  switch(config-if)# ip access-group abc
  ```

- CSCee89946

  Symptom: This caveat applies to Release 1.1(1) up to, and including, Release 1.3(4b). The Fibre Channel port link reinitialization sequence triggered by a link down event does not succeed if the switching module is up for more than 248 days and the last shutdown command on that port was issued 248 days prior to the link failure. After the link-down event, the port remains in the link failure or not connected state as shown in the following command output:

  ```
  switch# show interface fc2/1
  fc2/1 is down (Link failure or not-connected)
  ```

  Workaround: Issue the shutdown command, followed by the no shutdown command, on the affected port to bring the port back to link-up state as shown in the following command output:

```
switch# config t
switch(config)# interface fc2/1
switch(config)# shutdown
switch(config)# no shutdown
```

Issue the following commands to verify the module uptime.

```
switch# attach module 2
Attaching to module 2 ...
```

To exit type **exit**, to abort type **$**.

```
module-2# show version
Software
BIOS:      version 1.0.8
system:    version 2.0(1) [build 2.0(0.139)]
BIOS compile time:       08/07/03
system compile Time:     10/25/2020 12:00:00
Hardware
RAM 186668 kB
bootflash: 125184 blocks (block size 512b)
lc02   uptime is 11 days 18 hours 18 minute(s) 9 second(s)
```

Other notes:

- Any nondisruptive upgrade or downgrade resets the 248-day window.
- Once the shutdown and no shutdown commands are issued, it is good for another 248 days.
- If the switch has been up for a long time and the customer wants to connect new devices to the switch ports, then you may start with the shutdown and no shutdown commands on those ports

- CSCeg61535

  Symptom: The Telnet server may not be disabled even if you disable it through setup. A telnet session will still work in the switch.

  Workaround: Issue the **no telnet server enable** command in configuration mode to disable telnet after you login to the switch.

- CSCeh21199

  Symptom: If the NetApp file server appliance is configured as an initiator performing a Network Data Management Protocol (NDMP) backup, then the fabric login (FLOGI) process on the MDS switch might terminate because of excessive LSTS requests.

  This might happen if your N port or NL port uses extended link services to manage and control a public remote loop. The NetApp file server appliance configuration uses these services, namely LSTS and LINIT, which are documented in the Fibre Channel standards compliance (FC-FLA standard) specification.

  Workaround: Upgrade to Cisco MDS SAN-OS Release 2.0(4).

Related Documentation

Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family

Cisco MDS 9100 Series Quick Start Guide

Cisco MDS 9500 Series and Cisco MDS 9216 Quick Start Guide

Cisco MDS 9100 Series Hardware Installation Guide

Cisco MDS 9216 Switch Hardware Installation Guide

Cisco MDS 9500 Series Hardware Installation Guide

Cisco MDS 9000 Family Command Reference

Cisco MDS 9000 Family Configuration Guide

Cisco MDS 9000 Family Fabric Manager User Guide

Cisco MDS 9000 Family Troubleshooting Guide

Cisco MDS 9000 Family System Messages Guide

Cisco MDS 9000 Family MIB Reference Guide

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/univercd/home/home.htm

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to mdsfeedback-doc@cisco.com.

You can submit comments 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 can perform these tasks:

- 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 and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from 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 might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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)—Your 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 operation 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 your network is impaired, but 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.

- Cisco Marketplace provides a variety of Cisco books, reference guides, 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

- *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

- 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.