Send documentation comments to mdsfeedback-doc@cisco.com.

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

Release Date: September 28, 2005

Text Part Number: OL-7411-04

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 15.

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

Contents

This document includes the following sections:

- Introduction, page 2
- System Requirements, page 2
- Image Upgrade, page 5
- New Features in Cisco MDS SAN-OS Release 2.1(2b), page 6
- Limitations and Restrictions, page 6
- Caveats, page 7
- Related Documentation, page 15
- Obtaining Documentation, page 16
- Documentation Feedback, page 17
- Cisco Product Security Overview, page 17
- Obtaining Technical Assistance, page 18
- Obtaining Additional Publications and Information, page 19

Cisco Systems

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

Introduction

The Cisco MDS 9000 Family of multilayer directors and fabric switches offers intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. These switches 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 2.1(2b) and includes the following topics:

- Components Supported, page 2
- Determining the Software Version, page 5

Components Supported

Table 1 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 1 Cisco MDS 9000 Family Supported Software and Hardware Components

Component	Part Number	Description	Applicable Product
Software	M95S1K9-2.1.2B	MDS 9500 Supervisor/Fabric-I, SAN-OS software.	MDS 9500 Series only
	M92S1K9-2.1.2B	MDS 9216 Supervisor/Fabric-I, SAN-OS software.	MDS 9200 Series only
	M91S1K9-2.1.2B	MDS 9100 Supervisor/Fabric-I, SAN-OS software.	MDS 9100 Series only

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
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
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-C9120-K9	MDS 9120 fixed configuration, non-modular, fabric switch (includes 4 full rate ports and 16 host-optimized ports).	MDS 9120 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

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
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.	
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]	CWDM-SFP-xxxx-2G	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
	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	300-W[3] AC power supply.	MDS 9100 Series only
	DS-CAC-845W	845-W AC power supply.	MDS 9200 Series only
	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.	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB.	MDS 9500 Series only

Table 1 Cisco MDS 9000 Family Supported Software and Hardware Components (continued)

Component	Part Number	Description	Applicable Product
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.

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

When downgrading from Cisco MDS SAN-OS Release 2.1(2b) to Release 1.3(x), you might need to disable new features in Release 2.1(2b) 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 that the downgrade is disruptive and the reason is “current running-config is not supported by new image.”

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
      2       yes      disruptive         reset  Current running-config is not
supported by new image
      3       yes      disruptive         reset  Current running-config is not
supported by new image
      5       yes      disruptive         reset  Current running-config is not
supported by new image
      6       yes      disruptive         reset  Current running-config is not
supported by new image
```

At a minimum, you need to disable the default device alias distribution feature using the **no device-alias distribute** command in global configuration mode. The **show incompatibility system bootflash:1.3(x)_filename** command determines which additional features need to be disabled.

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

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

The new features for this release are the same as those listed in the *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 2.1(2).*

Limitations and Restrictions

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

IVR

All IVR enabled switches in a network must be either in NAT or non-NAT mode. Mixing the two modes is not supported. Ensure that a switch with IVR-NAT mode enabled never coexists in the network with another switch where IVR is enabled without NAT mode enabled.

While migrating from IVR non-NAT mode to NAT mode in Cisco MDS SAN-OS Release 2.1(1b), deactivate the IVR zoneset, disable IVR on all of the IVR enabled switches, then reenable IVR. Finally, enable NAT mode and then the IVR configurations. Note that migration between the non-NAT and NAT modes is disruptive to IVR traffic and the FCIDs of the IVR devices change in the exported VSANs.

While upgrading the SAN-OS images on IVR enabled switches, upgrade all of the IVR enabled switches to the new SAN-OS version before making any topology or configuration changes.

CFS distribution for IVR should be disabled on all IVR enabled switches before upgrading from Cisco MDS SAN-OS Release 2.0(x) to Releases 2.1(1b) or 2.1(2b). After upgrading all of the IVR-enabled switches to Cisco MDS SAN-OS Release 2.1(1b) or Release 2.1(2b), CFS distribution for IVR can be reenabled.

14/2-Port Multiprotocol Services Module

The MPS-14/2 module does not support a MTU size greater than 8000 bytes. An attempt to set the MTU size greater than 8000 bytes will result in an error. Reset the MTU size value between 576 to 8000 bytes and issue the no shutdown command on the port for normal operation.

Caveats

This section lists the open and resolved caveats for this release. Use Table 2 to determine the status of a particular caveat. In the table, “O” indicates an open caveat and “R” indicates a resolved caveat.

Table 2 Open Caveats and Resolved Caveats Reference

	Software Release (Open or Resolved)	
DDTS Number	2.1(2)	2.1(2b)
Severity 2		
CSCeg90336	O	O
CSCeh52973	O	O
CSCeh73149	O	O
CSCeh92604	O	O
CSCeh93109	O	O
CSCei10774	O	O
CSCei18449	O	R
CSCei18830	O	O
CSCei19822	O	O
CSCei40874	O	O
CSCei50818	O	R
CSCei53783	O	O
CSCei55341	O	O
CSCei62511	O	R
CSCei73996	O	R
CSCei81840	O	R
CSCei82417	O	R
CSCei88345	O	R
Severity 3		
CSCec31365	O	O
CSCed16845	O	O
CSCef56229	O	O
CSCeg12383	O	O
CSCeg27584	O	O
CSCeg37598	O	O
CSCeg55238	O	O
CSCeh33548	O	O
CSCeh34828	O	O
CSCeh41099	O	O
CSCeh75500		O

Table 2 Open Caveats and Resolved Caveats Reference (continued)

	Software Release (Open or Resolved)	
DDTS Number	2.1(2)	2.1(2b)
CSCeh88814	O	O
CSCei32317	O	O
CSCei48889	O	O
CSCei67982	O	R
CSCei76309		R
CSCei77038	O	R
CSCei78778	O	R
CSCei83322		O
CSCin92870		O
CSCin95686		O
CSCin95789		O

Resolved Caveats

- CSCei18449

  Symptom: When upgrading from Cisco MDS SAN-OS Releases 2.1(1x) to 2.1(2x), in some circumstances, the SSM or ASM modules might not boot properly after the install all command is issued.

  Workaround: Manually reload the SSM or ASM module.

- CSCei50818

  Symptom: iSCSI hosts are unable to log in to the target storage arrays because of name server issues on the IPS blade.

  Workaround: None.

- CSCei62511

  Symptom: If the Cisco MDS 9020 switch has a large number of zones defined, the Fabric Manager will not display them because of buffering requirements.

  Workaround: None.

- CSCei73996

  Symptoms: Under certain circumstances, Fabric Mananger shows cached zone members.

  Workaround: None.

- CSCei79457

  Symptom: The port manager process fails because of a NULL pointer access causing a system switchover during a long testing cycle.

  Workaround: None.

- CSCei81840

Symptom: Even though FCIP IVR capability on a Cisco MDS 9216i switch is bundled with hardware at no extra charge, a switch running Cisco MDS SAN-OS Release 2.1(1a) or later might disable FCIP IVR functionality after the 120 days of enabling the feature. As a result, the Cisco MDS 9216i switch will stop routing traffic, such as IVR functionality, over the FCIP links. There are no issues if FCIP functionality is not enabled on the Cisco MDS 9216i switch.

Workaround: Contact your OSM and/or Cisco TAC to obtain and install SAN-OS version 2.1.2b. If you are unable to upgrade to SAN-OS 2.1.2b at this time, then work with your OSM's service organization to obtain and install a software fix.

- CSCei82417

  Symptom: When multiple roles are configured on the switch, the SNMP process may consume more memory if the user logs in using the GUI with some VSAN restrictions.

  Workaround: Use the network-admin role only, the CLI only, or two well defined roles, network-admin and network-operator.

- CSCei88345

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

  – FCIP connection flapping during the upgrade process resulting in fabric segmentation or merge.

  – ISL flap results in fabric segmentation or merge because of hardware issues or a software bug.

  – ISL port becomes part of PCP results in fabric segmentation or merge because of a port flap.

  If this problem occurs, syslogs indicate RDI failure and the flapped lSL could remain in a down state because of a domain overlap. This is caused by conflicts between the allowed domains list and the virtual domain requested through RDI.

  Workaround: There are four distinct scenarios for which the workarounds are provided.

1. If you are running Cisco MDS SAN-OS Releases 1.3(X) or 2.0(X) with IVR enabled, we recommend upgrading to Release 2.0(2b). Please contact your OSM for 2.1(2b) availability.
2. If you have already upgraded some or all of your Cisco MDS SAN-OS switches from Cisco MDS SAN-OS Release 1.3(X) or 2.0(x) to Release SAN-OS 2.1(1a), 2.1(1b), or 2.1(2a), a scheduled downtime is required to perform the following steps:

   a. Configure static domains for all switches in all VSANs where IVR is enabled. Configure the static domain the same as the running domain so that there is no change in domainIDs. Make sure that all domains are unique across all of the IVR VSANs. We recommend this step as a best practice for IVR-non-NAT mode.

      Issue the fcdomain domain {id} static vsan {vsan id} command to configure the static domains.

   Note Complete Step 2a for all switches before moving to Step 2b.

   b. b. Issue the no ivr virtual-fcdomain-add vsan-ranges 1-4093 command to disable RDI mode on all IVR enabled switches. This can cause traffic disruption.

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

   c. Check the syslogs for any ISL that was brought down.

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

d. Identify any switches isolated and issue the following commands for the affected switches:

```
switch(config)# vsan database
switch(config-vsan-db)# vsan {vsan ID} suspend
switch(config-vsan-db)# no vsan {vsan ID} suspend
```

e. e. Issue the ivr refresh command to perform an IVR refresh on all the IVR enabled switches.

f. f. Issue the copy running startup command to save the RDI mode in the startup configuration on all of the switches.

3. If you have already upgraded some or all of the switches from Cisco MDS SAN-OS Release 1.3(X) or 2.0(x) to Releases 2.1(1a), 2.1(1b), or 2.1(2a), with Interop-mode 2 or 3 enabled, issue the **ivr refresh** command to perform the IVR refresh on all the IVR enabled switches.

4. If you are adding new switches running Cisco MDS SAN-OS Releases SAN-OS 2.1 (1a), 2.1(1b), or 2.1 (2a) to your existing network running Releases 1.3(X) or 2.0 (X), disable RDI mode on your new switches before adding them to the existing network. Issue the no ivr virtual-fcdomain-add vsan-ranges 1-4093 command to disable RDI mode.

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

- CSCei67982

  Symptoms: During an upgrade of a Cisco MDS 9000 Family switch with two or more MPS 14/2 modules, FCIP tunnels on multiple MPS 14/2 modules can be down at the same time. If a PortChannel with two FCIP tunnels on different 14+2 modules is used for redundancy, this redundancy can be lost. If IVR is running over these FCIP tunnels, IVR can lose remote devices as a result of loss of access over the FCIP-based PortChannel.

  Workaround: Place other hitless upgradeable modules between the 14+2 modules to allow for more time between module upgrades and give the FCIP tunnels more time to stabilize.

- CSCei76309

  Symptoms: Using the Software Install Wizard to install a mix of FabricWare and SANOS software will not work. Once you select SANOS (even if you unselect later), it removes the Fabricware ability.

  Workaround: None.

- CSCei77038

  Symptoms: If you use Device Manager to configure the radius server, the Cisco MDS 9020 switch does not send an authorization request to the server. When configured from the CLI, it works fine.

  Workaround: None.

- CSCei78778

  Symptom: If you restrict the user from changing interface parameters, the user might be able to change it in the running configuration using Device Manager until the changes are saved in the startup configuration.

Workaround: The SAN switch administrator can login in to Device Manager as a restricted user, change the switch port mode, then revert back to the previous mode, then exit Device Manager. This prompts the user to save the configuration to startup configuration, but it will fail or work based on the user roles. After this procedure, a restricted user may not be able to change the switchport mode.

Open Caveats

- CSCeg90336

  Symptom: A user that you created using Fabric Manager or Device Manager cannot log in from the console. Release 2.1(2) fixes this problem. However, if a third-party application creates a user using SNMP, a new MIB is required for Release 3.0.

  Workaround: Third-party applications should use SSH to connect to the MDS 9000 switch, and then use CLI commands to create the user account.

- CSCeh52973

  Symptom: The switch appears in two VSANs when connected through an Inter-Switch Link (ISL).

  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.

- CSCeh93109

  Symptom: If SANTap is unprovisioned before the appliance deletes the objects it had previously created, then SANTap might have problems with the session objects that are present.

  Workaround: The appliance must delete all objects first before SANTap is unprovisioned.

- CSCei10774

  Symptom: Disabling QoS does not remove the QoS attribute from an IVR zone set, and subsequent activation of the IVR zone set will not succeed.

Workaround: Remove the QoS attribute from the IVR zone set, both active and configured, before disabling QoS.

- 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.

- CSCei40874

  Symptom: If port 9001 is in use by another process, the database update for the previous release tables and data may hang.

  Workaround: Edit the server.properties file in the bin directory and use another port. Alternatively, remove the process that opened port 9001.

- CSCei53783

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

  Workaround: None.

- CSCei55341

  Symptom: Undefined objects are found in CISCO-VLAN-MEMBERSHIP-MIB.

  Workaround: None.

- CSCec31365

  Symptom: When IVR is enabled, the Fabric-Device Management Interface information is not transferred across VSANs for IVR devices.

  Workaround: None.

- CSCed16845

  Symptom: Occasionally, the Common Information Model (CIM) server may be automatically restarted because of an internal error. In this case, the connected CIM client is disconnected.

  Workaround: You must explicitly reconnect the CIM client to the CIM server.

- 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.

- CSCeg12383

  Symptom: On rare occasions, the PortChannels with FCIP interface members fail to come up when the switch reboots. This happens when the startup configuration has a default switch port trunk mode setting that does not match the configured trunk mode for PortChannel members (FCIP interfaces). Also, the startup configuration shows any explicit switch port trunk mode setting for the PortChannel.

  Workaround: Reconfigure the switch port trunk mode on the PortChannel.

- 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.

- CSCeg55238

  Symptom: Files created using the fcanalyzer local command cannot be copied or viewed. FC analyzer runs as root and the files that it creates are created with the owner as root. The correct file creation masks are not set when the file is created and so no user other than root can read or copy the file.

  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.

- CSCeh34828

  Symptom: If there are active IVR zones with the QoS attribute, then QoS should not be disabled (for example, with the no qos enable command or through Fabric Manager).

  Workaround: Before disabling QoS, QoS attributes from the active IVR zones should be removed and then the resultant IVR zone set should be reactivated.

- 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 trafffic (such as ICMP ping) sent by the Microsoft host in clear text will be dropped in the MDS port.

Workaround: None.

- 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.

- CSCei48889

  Symptom: LTO-1 tape drives in certain tape libraries can not be used with NASB feature. When multiple initiators (such as Backup Host and NASB engine) issue SCSI write commands, the tape drives respond with a SCSI CHECK CONDITION with Sense - 0x03 and ASC/ASCQ = 0x3b/0x00. They do not handle the transition from the host initiator to the NASB engine initiator. In general, this is an issue for all NASB solutions with this tape drive and library combination.

  Workaround: None.

- CSCei83322

  Symptom: VPM does not start after an update to Cisco MDS SAN-OS Release 2.1(2) on the SSM module. The module remains in a power cycled state.

  Workaround: Power down all ASM and SSM modules on the switch and power them back. This causes the VPM process to start. Issue the show processes | include vpm command to ensure the process started.

- CSCin92870

  Symptom: The Fabric Manager Server does not automatically handle a fabric merge and split. As a result, you many see duplicate fabrics in the database and the web client.

  Workaround: Close all fabrics from the Fabric Manager Server and then reopen the new fabric.

- 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.

Related Documentation

The documentation set for the Cisco MDS 9000 Family includes the following documents:

- *Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Releases*
- *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 VERITAS Storage Foundation for Networks Software*
- *Cisco MDS SAN-OS Compatibility Matrix for Storage Service Interface Images*
- *Cisco MDS 9000 Family SSM Configuration Note*
- *Cisco MDS 9000 Family ASM Configuration Note*
- *Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family*
- *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 MDS 9000 Family Software Upgrade and Downgrade Guide*
- *Cisco MDS 9000 Family Configuration Guide*
- *Cisco MDS 9000 Family Command Reference*
- *Cisco MDS 9020 Fabric Switch Configuration Guide and Command Reference*
- *Cisco MDS 9000 Family Fabric Manager Configuration Guide*
- *Cisco MDS 9000 Family Fabric and Device Manager Online Help*
- *Cisco MDS 9000 Family SAN Volume Controller Configuration Guide*
- *Cisco MDS 9000 Family Quick Configuration Guide*
- *Cisco MDS 9000 Family Fabric Manager Quick Configuration 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*
- *Cisco MDS 9000 Family Troubleshooting Guide*
- *Cisco MDS 9000 Family Port Analyzer Adapter 2 Installation and Configuration Note*

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

For information on VERITAS Storage Foundation™ for Networks for the Cisco MDS 9000 Family, refer to the VERITAS website: http://support.veritas.com/

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/

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

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

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same 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=) from Cisco Marketplace at this URL:

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

Ordering Documentation

Beginning June 30, 2005, 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/

Send documentation comments to mdsfeedback-doc@cisco.com.

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 send comments about Cisco documentation to bug-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

  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.

- 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 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 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.

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)—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, 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.

Send documentation comments to mdsfeedback-doc@cisco.com.