



Global Distributed Storage Engineering
Citi Architecture and Technology Engineering

Cisco MDS SAN Switch

GDSE-07002-SG
Solutions Guide

1.1

Version Control

Version	Date	Author	Reviewed	Comments
0.1	8-Feb-07	Parul Jain	Global Stakeholders	ML1 RFC
0.2	6-Mar-07	Parul Jain	Global Stakeholders	ML2 RFC
0.3	26-Mar-07	Parul Jain	Global Stakeholders	ML3 RFC
0.6	15-Aug-07	Parul Jain	Global Stakeholders	ML4-10 RFC
1.0	26-Oct-07	Parul Jain	Global Stakeholders	RFC
1.1	21-Nov-07	Parul Jain	Global Stakeholders	Release

Table Of Contents

1. INTRODUCTION.....	6
2. FABRIC DESIGN GUIDE	6
2.1. CERTIFIED MODELS AND SOFTWARE VERSIONS.....	6
2.2. COMMON HARDWARE AND SOFTWARE REQUIREMENTS.....	6
2.3. FABRIC TOPOLOGIES.....	6
2.3.1. SINGLE TIER (ALSO CALLED COLLAPSED CORE)	7
2.3.2. TWO TIER (ALSO CALLED EDGE-CORE)	7
2.3.3. DUAL FABRICS	7
2.4. SCALABILITY CONSIDERATIONS	7
2.5. ISL DESIGN BEST PRACTICES	8
2.6. FRONT END OVERSUBSCRIPTION	9
2.6.1. DEDICATING BANDWIDTH	10
2.7. SLOT RESERVATION FOR FUTURE FUNCTIONALITY	10
2.8. TAPE SANS	10
2.9. FABRIC DESIGN EXAMPLES	11
2.9.1. SINGLE TIER WITH MDS 9506	11
2.9.2. SINGLE TIER WITH MDS 9509	11
2.9.3. SINGLE TIER WITH MDS 9513	12
2.9.4. TWO TIER WITH SINGLE CORE AND 2GBPS STORAGE PORTS	12
2.9.5. TWO TIER WITH DUAL CORES AND 2GBPS STORAGE PORTS.....	13
2.9.6. TWO TIER WITH DUAL CORES AND 4GBPS STORAGE PORTS.....	14
3. PHYSICAL INSTALL CONSIDERATIONS	15
3.1. RACK	15
3.2. POWER AND COOLING.....	16
3.3. ETHERNET AND CONSOLE CONNECTIONS	16
3.4. KEEP FAN TRAY CLEAR!.....	16
3.5. POWER SUPPLY CIRCUITS.....	16
4. FABRIC/SWITCH MANAGEMENT INFRASTRUCTURE	16
4.1. ARCHITECTURE	16
4.2. MANAGEMENT SERVER SIZING AND PLACEMENT	18
4.3. TERMINAL SERVICES LICENSE.....	19
5. MANAGEMENT SERVER BUILD	19
5.1. STEP 1: CHECK FOR JRE	19
5.2. STEP 2: INSTALL FABRIC MANAGER	19
5.3. STEP 3: SECURE FABRIC MANAGER SERVER.....	20
5.4. STEP 4: SECURE PERFORMANCE MANAGER SERVER	20
5.5. STEP 5: INSTALL SSH CLIENT	21
5.6. STEP 6: INSTALL SFTP SERVER	21
5.7. STEP 7: CONFIGURE FMS WITH CITI SSH	21
5.8. STEP 8: CONFIGURE CALL-HOME	24
5.8.1. CALL-HOME TO EMC	24
5.8.2. CALL-HOME TO HDS.....	25
5.9. STEP 9: CONFIGURE FMS TO AUTHENTICATE TO ACTIVE DIRECTORY.....	26

5.10.	STEP 10: MANAGEMENT SERVER ACCESS CONTROL	27
5.11.	STEP 11: REBOOT THE SERVER.....	27
6.	SWITCH CONFIGURATION STEPS.....	27
6.1.	STEP 1: DESIGN VSAN IDS AND DOMAIN IDS	27
6.2.	STEP 2: DESIGN NAMING.....	29
6.3.	STEP 3: CUSTOMIZE CONFIGURATION TEMPLATE.....	29
6.4.	STEP 4: POWER UP AND FIRST LOGIN	29
6.5.	STEP 5: CONFIGURE IP ADDRESS & DEFAULT GATEWAY	30
6.6.	STEP 6: UPGRADE SANOS TO GDSE CERTIFIED VERSION	30
6.7.	STEP 7: COPY CONFIGURATION SCRIPT FROM STEP 3 TO SWITCH FILESYSTEM.....	31
6.8.	STEP 8: RUN THE CONFIGURATION SCRIPT.....	31
6.9.	STEP 9: OBTAIN AND INSTALL LICENSING	31
7.	USER IDS AND AUTHENTICATION.....	32
7.1.	INTERACTIVE AUTHENTICATION	32
7.2.	PURPOSE OF NETWORK-ADMIN ROLE	37
7.3.	NON-INTERACTIVE AUTHENTICATION.....	38
8.	AUDIT TRAIL MANAGEMENT.....	40
9.	VENDOR REMOTE ACCESS.....	41
10.	INTEGRATION WITH ECC	43
11.	INTEGRATION WITH SANSCREEN	44
12.	MONITORING THE SWITCH WITH ESS.....	44
12.1.	IMPLEMENTATION STEPS.....	45
12.2.	TRAPS TO MONITOR	45
12.3.	TESTING.....	47
13.	INTEGRATION WITH ETRUST AUDIT	48
14.	PORT SECURITY	48
15.	BACKUP AND RECOVERY	49
15.1.	SWITCH BACKUP AND RECOVERY.....	49
15.2.	MANAGEMENT SERVER BACKUP AND RECOVERY	49
16.	FIRMWARE UPGRADES.....	50
17.	KNOWN ISSUES	50
18.	APPENDIX A: PARTS LIST FOR SAMPLE FABRIC DESIGNS.....	52
19.	APPENDIX B: GLOSSARY	54
20.	APPENDIX C: RESOLVING APPLICATION CONFLICTS.....	56



20.1.	CONFIGURE PATH TO JAVA RUNTIME.....	57
20.2.	CONFIGURE TCP/UDP PORTS.....	58
21.	APPENDIX D: SWITCH CONFIGURATION (“TEMPLATE”).....	59
22.	APPENDIX E: ETRUST AUDIT MP FILE	66

1. Introduction

Cisco MDS Fibre Channel Switches are the new standard for building Storage Area Networks (SAN) at Citi. This Solutions Guide will aid global SAN operations teams in designing and deploying SANs based on MDS. For the latest version of this document and for other related documentation please visit the GDSE homepage for MDS at:

<http://engineering.citigroup.net/gdse/products/platforms/ciscomds/>

Please see appendix B for a description of terms used in this document.

2. Fabric Design Guide

2.1. Certified Models and Software Versions

Director Models	Cisco MDS 9506, 9509, 9513
Switch Model ¹	Cisco MDS 9124
SANOS Version	3.1.2
Supervisor	Supervisor 2
Line Cards	12, 24 and 48 port generation 2 line cards 14+2 MPSM line card for FCIP
Management Software	Fabric Manager 3.1.2 on SOE Windows 2003 Server ²

2.2. Common Hardware and Software Requirements

- All switches must be ordered with 2 Supervisor-2 modules
- All switches must be ordered with
 - Enterprise License – Required for advanced security features such as Port Security
 - Fabric Manager Server License – Required for performance monitoring and reporting

2.3. Fabric Topologies

GDSE has certified the use of the following fabric topologies for fabrics contained within the datacenter (“Local SAN”).

¹ This is being certified as a replacement for McData 4700 for very small SANs

² CLI access via SSH is supported from any platform

2.3.1. Single Tier (also called collapsed core)

The Cisco MDS family, especially the 9513, is a much higher density platform as compared to currently certified McData technology. Current single edge-core designs can be easily collapsed into a single tier. A single tier design has the advantage of not using any ISLs thereby reducing cost and complexity, and optimizing performance.

2.3.2. Two Tier (also called edge-core)

A core-to-edge fabric topology is recommended to provide any-to-any connectivity, evenly distribute traffic, maximize the ease of scalability and maintain a single hop between devices. In this topology, the core switch connects to tier 1 devices and to edge switches. The tier 1 devices are those requiring high bandwidth and availability such as storage arrays, media servers, streaming streamers, and tape devices. Servers should be attached to the edge switches.

Large SAN environments where a 9513 will still not meet the connectivity requirements should consider a 2-tier dual core dual fabric architecture. In this design, ISL's from all edge switches are connected to a pair of dual core switches in each fabric. Storage ports are evenly distributed between the pair of dual core switches in each fabric. While this approach increases the total ISL requirements, it effectively doubles the number of core ports available and maintains a single hop architecture. In large environments such as this, consideration should be given to the increased operational risk of having twice as many servers attached to the same SAN fabrics. Change management policy and procedures may need to be enhanced to reduce the risk of change affecting both large fabrics at the same time.

2.3.3. Dual Fabrics

Dual fabrics should be implemented to provide high availability. Storage arrays and servers should be dual connected to each of the fabrics. This provides increased bandwidth and two independent data paths. There is also protection from single path failure (HBA, cable, switch) and allows for non-disruptive maintenance of the combined SAN. The fabrics should be designed symmetrically for ease of management.

2.4. Scalability Considerations

Selection of switch model, topology and type of line cards should be based on the maximum number of host ports that the SAN will ever support. A good estimate of this number can be obtained by assessing the current host port need and then growing this by an annual increase estimate for the life of the equipment. For example, if there is a demand for 20 host ports today, and the demand is expected to grow by 25% each year, and technology refresh for this type of equipment happens every 5 years in your region, the fabric should be built for supporting 63 host ports.

2.5. ISL Design Best Practices

Cisco uses different terminology than McData for Inter-Switch Links. This document uses Cisco terminology throughout. Please see Appendix B, “Glossary”, for an explanation of terms and differences from McData terminology.

Unlike McData, all equal cost paths are load balanced using a source/destination/OXID hash. This load balancing is applied to load balance individual ISLs within a Port Channel, and to load balance Port Channels.

- Assume fan-in ratio on the storage ports to be 10:1. This is a rule of thumb and can be modified depending on performance requirements if known.
- Switches should be interconnected by Port Channels. Each Port Channel should have at least two member links (ISLs), and each Port Channel member link should come from a different line card. This way the Port Channel can survive a line card failure.
- Each Port Channel can be scaled to 16 member links, and that should provide enough bandwidth for most topologies. A second Port Channel should only be considered when the first is fully populated with 16 links. Having a bigger Port Channel is desirable over having multiple Port Channels because failure of a Channel causes disruptive FSPF convergence to be triggered unlike failure of a member link within a Channel.
- On the core switch, ISLs should always be run from full line rate 4 Gbps ports found on the 12 port line card. If 9506 or 9509 switches are being used on the edge, ISLs can terminate on 24 port or 48 port line cards after dedicating 4 Gbps bandwidth to the selected ports. Because smaller switches have a limited number of slots, dedicating two slots to 12 port line cards to run ISLs would be inefficient. Please note that dedicating bandwidth to one or more ports in a port group increases the oversubscription ratio for the rest of the ports in that port group. Oversubscription ratio should be managed by either taking ports out of service from that port group, or by distributing ISL ports between port groups, or both.
- The following can be used to calculate number of members in the Port Channel:

If number of host ports that will use this Port Channel is H, and each host connects with S Gbps speed, and the storage port fan-in ratio is F

Total port channel bandwidth required = $(H * S)/F$

Number of port channel members = $(H * S)/F/4$

Example: If there are 100 host ports operating at 2 Gbps and fan-in ratio is 10, number of members in the port channel = 5.

- The entire Port Channel should be provisioned upfront; although MDS allows for non-disruptive addition of members to the Port Channel, Operations may run out of ports by over-allocating ports to hosts, or may even forget to address Port Channel bandwidth as hosts are being added to the fabric.

2.6. Front End Oversubscription

Each slot on the MDS switch has around 51.2 Gbps of total bandwidth. That means each slot can support $51.2/4 = 12$ ports operating at full 4 Gbps. The 24 and 48 port line cards therefore have ports that share bandwidth.

	1 Gbps FC	2 Gbps FC	4 Gbps FC
12 port	Full rate	Full rate	Full Rate
24 port *	Full rate	Full rate	2 to 1 oversubscription
48 port *	Full rate	2 to 1 oversubscription	4 to 1 oversubscription

* Supports port bandwidth reservation

The sharing does not happen across all the ports on the line card; bandwidth is dedicated to “port groups” and ports within a port group share bandwidth.

Line Card	Ports Per Port Group	Bandwidth Per Port Group
48 port	12	12.8
24 port	6	12.8

Because of the fan-in ratio of 10:1 on the storage side, such sharing of bandwidth on the front end does not reduce the end-to-end bandwidth. However, because front end oversubscription is a new technology for Citi, judgment should be used in selecting hosts to connect to oversubscribed front end ports. Further, because Citi runs host and storage ports at 2 Gbps, front end oversubscription concerns are tied to the 48 port line card and not the 24 line card.

- The 48 port line card is recommended for host ports only. It should not be used for ISL, storage or tape ports
- Hosts (applications) that are known to generate high IO traffic all the time, such as media servers or streaming servers, should be provisioned on 24 port line cards
- In a mixed development and production environment, development hosts can be provisioned on 48 port line cards, and production on 24 line cards
- Port utilization on 48 port line cards should be continuously monitored using the Performance Manager. Utilization for 12 ports in the group should be aggregated to see if total group capacity of 12.8 Gbps is being reached on multiple occasions. If this is the case, hosts generating more traffic within the group should be moved to less utilized port groups, or moved to a 24 port line card. It is a good idea to have a 24 port line card with a few ports open to support such moves.

2.6.1. *Dedicating Bandwidth*

Certain oversubscribed front end ports from the 24 port and 48 port line cards can be dedicated bandwidth. This may be required when one or more less important applications in the port group occasionally generate high IO traffic and rob more important applications of bandwidth, in which case it is a good idea to set aside bandwidth for the important applications. Another use of this configuration is when the shared ports must be used for ISLs, in which case the ports must be guaranteed 4 Gbps of bandwidth.

Dedicating bandwidth to ports must be carefully planned and ports that are provided dedicated bandwidth should be distributed between port groups. As a best practice, using shared bandwidth ports for storage, tape and ISL should be avoided.

2.7. *Slot Reservation for Future Functionality*

The MDS supports extended functionality through modules that can be used in line card slots. Even if the functionality is not needed/certified today, slots must be reserved for such modules in the fabric design.

Module Name	Functionality	GDSE Position
Storage Services Module (SSM)	Intelligent Fabric Services: Virtualization (EMC Invista), SANTap, NASB and FCWA	GDSE has evaluated Invista and found that in its current form it is not ready for use within Citi. Regional teams that see a strong need for SANTap, NASB and FCWA should contact GDSE and reserve slots in their designs.
Multi Protocol Services Module (MPSM)	IP Services: FCIP for SAN extension	Brocade has announced that IPS product line will not be sold after 2007. GDSE has certified IP Services on MPSM. The current MPSM module ³ has 14 FC and 2 GigE ports. A newer version of the module is expected Q1 2008 that will have 18 FC and 4 GigE ports. At least 2 MPSMs are recommended for redundancy. Smaller sites can use two slots on the 9513, but larger sites that would need more than 4 GigE ports should build a separate physical fabric for SAN extension. Slots should be accordingly reserved.

2.8. *Tape SANs*

Because most fabrics run out of storage ports on the core as the SAN grows, GDSE recommends building separate physical fabrics for backup purposes. Smaller sites with predictable storage and tape port growth may share the disk fabrics with tape after partitioning the tape fabrics off into their own VSANs. Any tape traffic traversing ISLs should also be partitioned off by using VSAN trunking. If a core-edge topology is being used for disk fabric, the edge ports can be used to connect hosts to the tape SAN. In this case, a dedicated tape core should be used to connect tape devices. The tape core switch should be collocated with the disk edge switch(s) so that if the disk

³ The current SSM and MPSM modules are “generation 1” type line cards. Using a “generation 1” line card in the switch puts a limitation on the total number of ports that the switch can have. There can be a maximum of 252 indexes; each port uses an index, and the module itself uses 22 indexes.

fabric is running out of edge ports the tape edge ports can be conveniently migrated to the tape core.

2.9. Fabric Design Examples

The following examples are provided to aid Regional Operations teams in designing their fabrics. The examples assume a 3 year technology refresh cycle and 25% year over year growth in host port count. Please see appendix A for detailed parts lists needed to build each design. Please note that none of these designs consider reserving slots for SSM or MPSM modules.

2.9.1. Single Tier with MDS 9506

All designs use full line rate/non-blocking at 1 & 2Gbps and 2:1 oversubscribed at 4Gbps 24 port modules for host and storage.

Fabric A		Fabric B	
1 x MDS 9506 4 x 24 port LC		1 x MDS 9506 4 x 24 port LC	

Max port count = 96 per Fabric (Total SAN = 192 ports)

Max host = 86 at 2Gbps

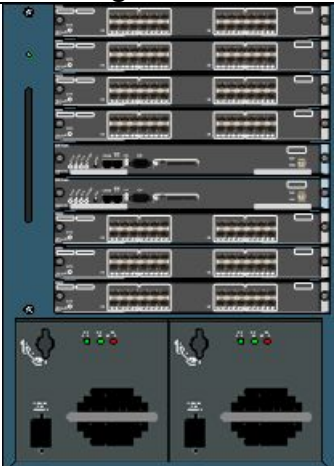
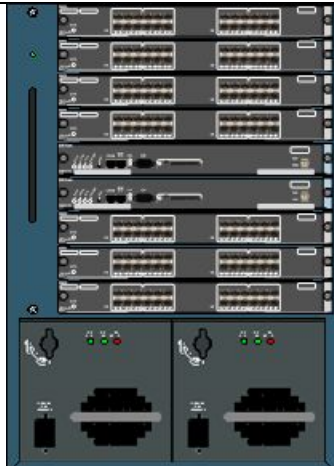
Max storage = 10 at 2Gbps

Host to Disk fan-in ratio of 8.6:1

Start		First year at 25%		Second year at 25%		Third year at 25%	
Host	Storage	Host	Storage	Host	Storage	Host	Storage
44	4	54	6	68	8	86	10

2.9.2. Single Tier with MDS 9509

All designs use full line rate/non-blocking at 1 & 2Gbps and 2:1 oversubscribed at 4Gbps 24 port modules for host and storage.

Fabric A		Fabric B	
1 x MDS 9509 7 x 24 port LC		1 x MDS 9509 7 x 24 port LC	

Max port count = 168 per Fabric (Total SAN = 336 ports)

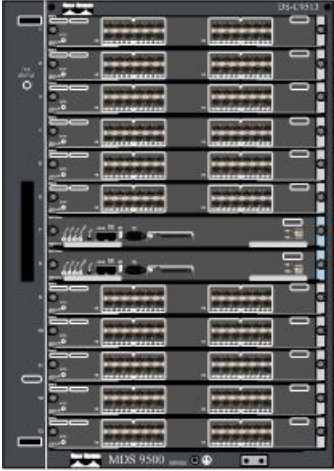
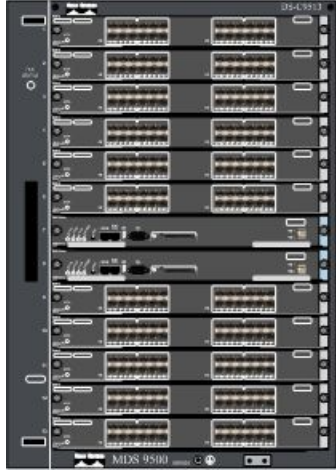
Max host = 152 at 2Gbps

Max storage = 16 at 2Gbps

Host to Disk fan-in ratio of 9.5:1

Start		First year at 25%		Second year at 25%		Third year at 25%	
Host	Storage	Host	Storage	Host	Storage	Host	Storage
78	8	98	10	122	12	152	16

2.9.3. Single Tier with MDS 9513

Fabric A		Fabric B	
1 x MDS 9513 11 x 24 port LC		1 x MDS 9513 11 x 24 port LC	

Max port count = 264 per Fabric (Total SAN = 528 ports)

Max host = 238 at 2Gbps

Max storage = 26 at 2Gbps

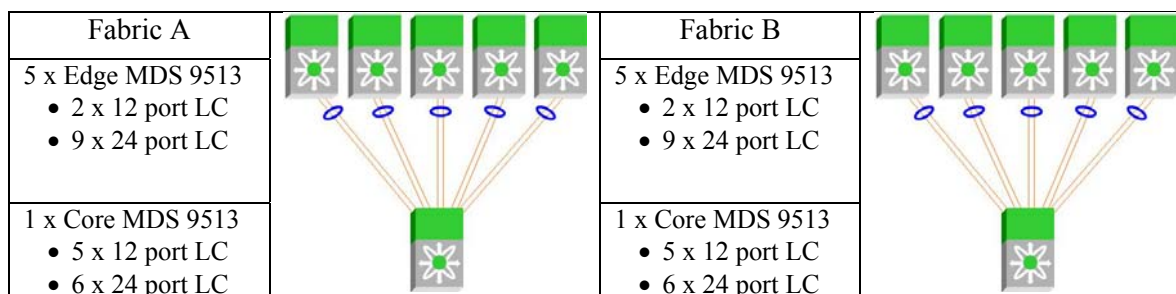
Host to Disk fan-in ratio of 9.1:1

Start		First year at 25%		Second year at 25%		Third year at 25%	
Host	Storage	Host	Storage	Host	Storage	Host	Storage
122	12	152	16	190	20	238	26

2.9.4. Two Tier with Single Core and 2Gbps Storage Ports

All designs use full line rate/non-blocking at 1 & 2Gbps and 2:1 oversubscribed at 4Gbps 24 port modules for host/storage and full line rate/non-blocking 1, 2, & 4Gbps 12 port modules for ISLs. The fabric can be built with one edge switch and one core switch, and then grown by adding edge switches⁴. Slots or 4 Gbps ports on the core switch must be reserved for ISLs to future edge switches. It is very common to run out of ISL ports on the core.

⁴ Addition of switches to the fabric is non-disruptive.



Max port count = 1404 per Fabric (Total SAN = 2808 ports)

Max Host = 1140 (1080 at 2Gbps and 60 at 4Gbps)

Max Storage = 144 at 2Gbps

ISL ports = 120 at 4Gbps

Host to Disk fan-in ratio of 8.3:1 and ISL fan-in ratio of 10:1

Port count per Edge switch

Max port count = 240

Max host = 228 (216 at 2Gbps and 12 at 4Gbps)

ISL = 12 at 4Gbps

ISL fan-in ratio = $480\text{Gbps} (216 \times 2\text{Gbps} + 12 \times 4\text{Gbps}) / 48\text{Gbps} (12 \times 4\text{Gbps}) = 10:1$

Port count per Core switch

Max port count = 204

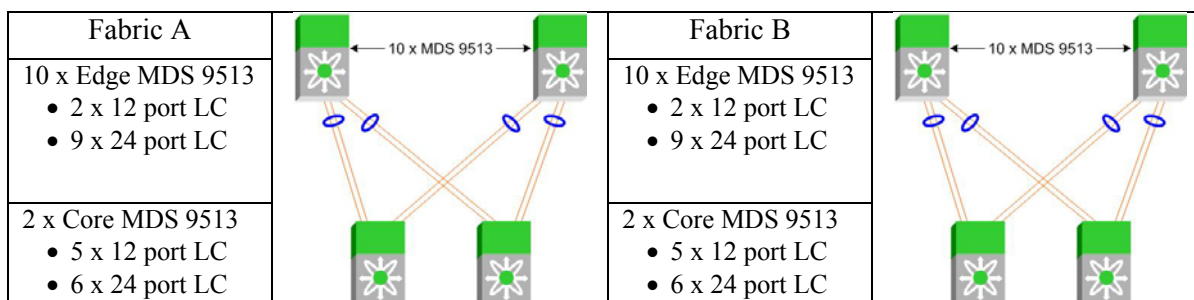
Max storage = 144 at 2Gbps

ISL = 60 at 4Gbps

Start		First year at 25%		Second year at 25%		Third year at 25%	
Host	Storage	Host	Storage	Host	Storage	Host	Storage
584	72	730	90	912	114	1140	144

2.9.5. Two Tier with Dual Cores and 2Gbps Storage Ports

All designs use full line rate/non-blocking at 1 & 2Gbps and 2:1 oversubscribed at 4Gbps 24 port modules for host/storage and full line rate/non-blocking 1, 2, & 4Gbps 12 port modules for ISLs. GDSE recommends that both core switches in the fabric should be deployed together, rather than starting with one core and adding the second one later. This is because storage port traffic must be balanced on both cores for optimal use of the ISL bandwidth in the dual-core. Uneven traffic distribution would require more ports to be dedicated for ISL reducing the benefit of having a second core. Slots or 4 Gbps ports on the core switches must be reserved for ISLs to future edge switches. It is very common to run out of ISL ports on the cores.



Max port count = 2808 per Fabric (Total SAN = 5616 ports)

Max Host = 2280 (2160 at 2Gbps and 120 at 4Gbps)

Max Storage = 288 at 2Gbps

ISL ports = 240 at 4Gbps

Host to Disk fan-in ratio of 8.3:1 and ISL fan-in ratio of 10:1

Port count per Edge switch

Max port count = 240

Max host = 228 (216 at 2Gbps and 12 at 4Gbps)

ISL = 12 at 4Gbps (6 per Core MDS 9513)

ISL fan-in ratio = 480Gbps (216*2Gbps + 12*4Gbps) / 48Gbps (12*4Gbps) = 10:1

Port count per Core switch

Max port count = 204

Max storage = 144 at 2Gbps

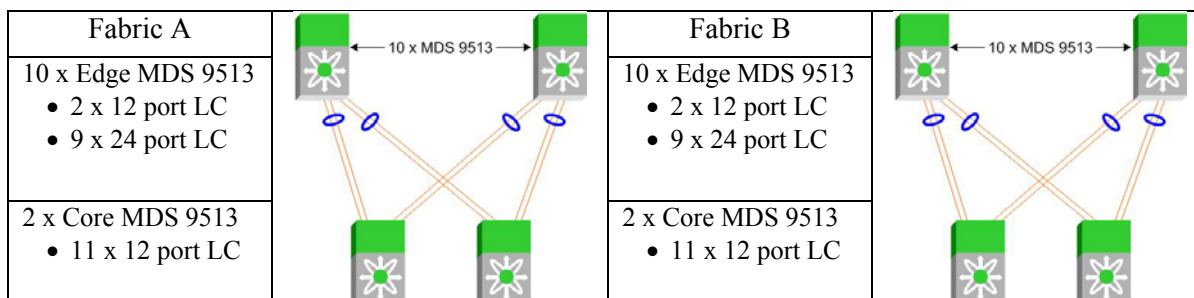
ISL = 60 at 4Gbps

Start		First year at 25%		Second year at 25%		Third year at 25%	
Host	Storage	Host	Storage	Host	Storage	Host	Storage
1168	148	1460	184	1824	230	2280	288

2.9.6. Two Tier with Dual Cores and 4Gbps Storage Ports

This is the GDSE recommended design for new datacenters.

All designs use full line rate/non-blocking at 1 & 2Gbps and 2:1 oversubscribed at 4Gbps 24 port modules for host and full line rate/non-blocking 1, 2, & 4Gbps 12 port modules for ISLs and Storage.



Max port count = 2664 per Fabric (Total SAN = 5328 ports)

Max Host = 2280 (2160 at 2Gbps and 120 at 4Gbps)

Max Storage = 144 at 4Gbps

ISL ports = 240 at 4Gbps

Host to Disk fan-in ratio of 8.3:1 and ISL fan-in ratio of 10:1

Port count per Edge switch

Max port count = 240

Max host = 228 (216 at 2Gbps and 12 at 4Gbps)

ISL = 12 at 4Gbps (6 per Core MDS 9513)

ISL fan-in ratio = $480\text{Gbps} (216 \times 2\text{Gbps} + 12 \times 4\text{Gbps}) / 48\text{Gbps} (12 \times 4\text{Gbps}) = 10:1$

Port count per Core switch

Max port count = 132

Max storage = 72 at 4Gbps

ISL = 60 at 4Gbps

Start		First year at 25%		Second year at 25%		Third year at 25%	
Host	Storage	Host	Storage	Host	Storage	Host	Storage
1168	74	1460	92	1824	115	2280	144

3. Physical Install Considerations

3.1. Rack

The Cisco MDS can either be installed in EMC provided cabinets, or customer provided 2 or 4 post rack as per the following table. HDS does not currently offer cabinets for the MDS, and therefore if switches are purchased from HDS they must be installed in customer provided racks. Because Citi is planning to procure MDS from either vendor, **GDSE recommends using racks (not EMC's cabinet) to have a standardized environment.**

Rack Type	MDS 9513	MDS 9509	MDS 9506
EMC Model	ED-1700-C	ED-1500-C	ED-1500-C
EIA (4-Post)	Yes	Yes	Yes
Telco (2-Post)	No	No	Yes

At most two MDS 9513s can be installed in a EIA 4 post rack. A fully loaded 9513 can weigh up to 375 lb, and Cisco recommends that a mechanical lift be used to install the fully loaded switch in the rack.

Cisco recommends that you maintain a minimum air space of 2.5 inches (6.4cm) between walls and the chassis air vents and a minimum horizontal separation of 6 inches (15.2 cm) between two chassis to prevent overheating.

It is a common mistake to order the wrong type of power cables that will not go into the power outlets on the rack. Locking type power connectors are preferred.

3.2. Power and Cooling

A 9513, fully loaded with 24 port line cards will consume around 2250 Watts of power. That is about 8.5 Watts of power per port. Compare this to currently certified McData Intrepid 6140 director, which consumes 842 Watts for 140 ports, which is about 6 Watts per port. The MDS will generate 36.4 BTU/hr per port of heat, whereas the 6140 generates only 20.5 BTU/hr per port. The extra power and cooling requirements should be planned for.

3.3. Ethernet and Console Connections

The switch needs two 100 Mbps full duplex Ethernet connections, and two Cisco RS232 console connections going to a terminal server⁵. Unlike McData CTP, each MDS Supervisor uses its own Ethernet and Console connections. Although two Ethernet connections are used, the switch only needs one IP address.

3.4. Keep Fan Tray Clear!

On the 9513, 9509 and 9506 switches, there is a full height fan tray on the left of the switch. Whenever a fan fails, the entire tray has to be pulled out and replaced within 5 minutes. If the tray is not replaced within that time, the switch will shutdown to prevent damage to the circuitry. **It is very important that cables do not obstruct the removal and insertion of the fan tray.**

3.5. Power Supply Circuits

Each 9500 series switch comes with two power supply units, and each unit has two power connections. The best practice is to connect both connections of each power supply to the same power circuit, and each power supply to a different power circuit. This way if one power circuit fails, only one power supply will be impacted. Because the switch uses power supplies in a redundant fashion, failure of one power supply will not bring down the overall power supply capacity.

4. Fabric/Switch Management Infrastructure

4.1. Architecture

Please refer to the following figure. Unlike McData switches that are connected to the Common Extranet Platform (“CEP”), the MDS switches will be directly connected to the Citi corporate network, called Global Data Network (“GDN”). A corporate IP network connected Windows 2003 SOE server (“Management Server”) would be used to host software applications to manage

⁵ The console connections are required for (1) initial configuration of switch (2) recover from a bad ACL command (3) watch detailed firmware upgrade progress (4) recover from ACS related misconfiguration or outage



one or more MDS switches and fabrics. Although Cisco MDS management applications are Java based and can run on other platforms including Solaris, GDSE is certifying Windows because that opens up the possibility of using virtual servers instead of physical servers for cost reduction. Citi Storage Operations personnel will log on to this server from their SOE workstations using Windows Remote Desktop Client. SSH client on the Windows server and any other authorized servers can also be used to bring up a CLI session and to run scripts.

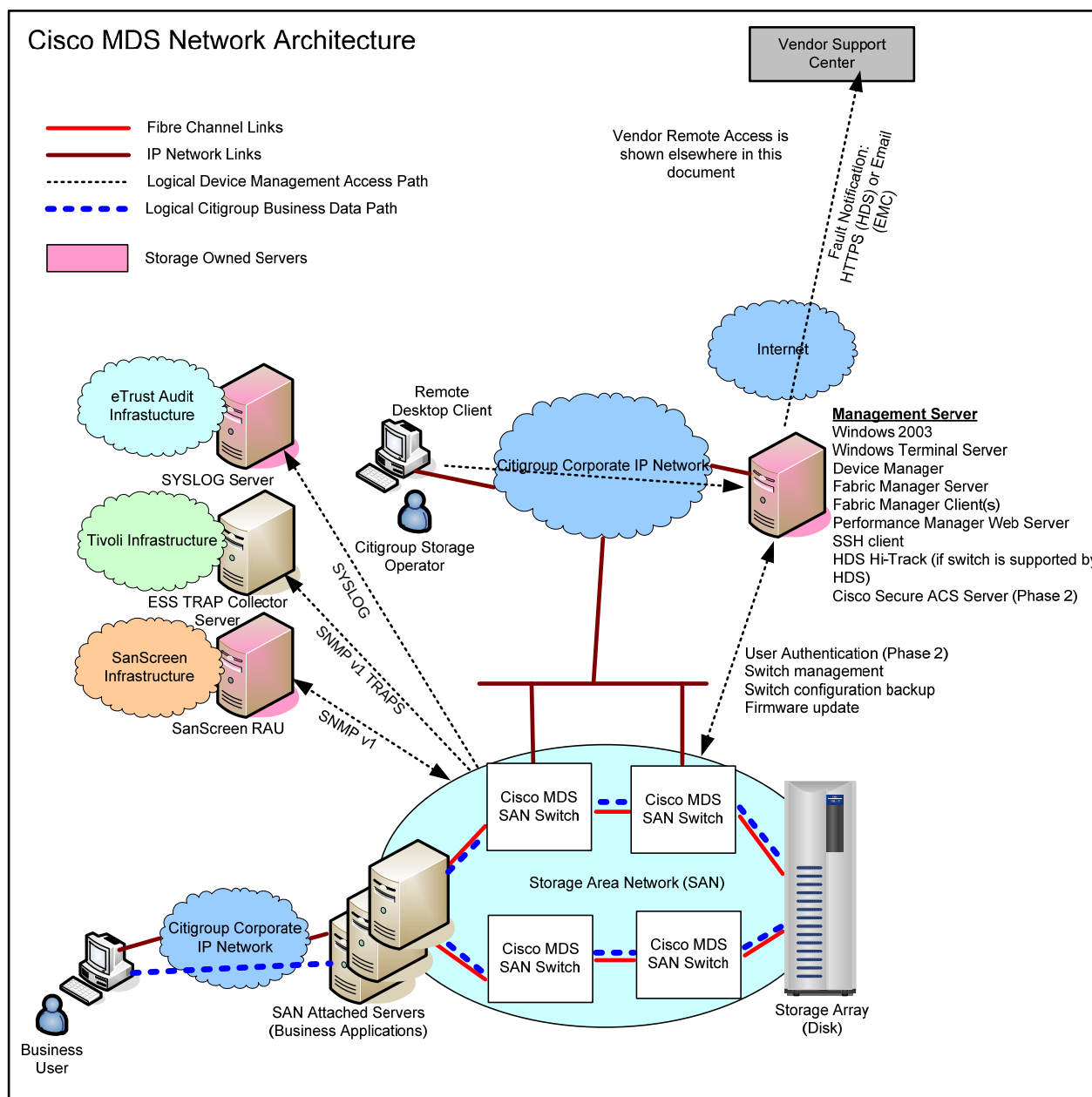
The switches will also interact with SYSLOG, ESS TRAP Collector, and SanScreen Remote Acquisition Unit (RAU) servers.

Syslog Server: GDSE recommends using a SOE Solaris server for capturing SYSLOG events emitted by the MDS switches. This is because the Solaris server already has a SYSLOG daemon that can do the job and GDSE has tested this configuration. Running a third party SYSLOG server on the Windows Management Server is an option, however there are three challenges with that approach:

1. There is not a certified SYSLOG server software for Windows SOE build
2. The Fabric Manager Server software itself uses UDP port 514 to listen to SYSLOG messages from the switches. This port cannot be reconfigured. In order for another SYSLOG server to run on the same server, the Management Server will have to be assigned a second IP address, and the SYSLOG server bound to that IP address. Alternatively, a different Windows server must be used.
3. GDSE has not tested this configuration

ESS Trap Collector Server: This server is a part of the ESS infrastructure.

SanScreen RAU Server: This is the server that runs the SanScreen RAU agent. Either an existing RAU server can be configured to additionally include the MDS switches, or the RAU agent can be installed on the Management Server itself.



4.2. Management Server Sizing and Placement

Managing fabrics across WAN links is not recommended because the GUI management applications interact with the switch in real time, and therefore user response is tightly linked to network performance. Each site should have its own Management Server. The same Management Server should be used for managing both A and B fabrics because Fabric Manager will not let the same administrator activate fabric A and B zonesets at the same time, thereby protecting from Operator errors during the most common change operation: zoning. There are no hard limits in the software for number of switches it can manage, but there are soft limits:

- 200 switches

- 5000 end devices
- 24 fabrics monitored

At least 2 GB of RAM is recommended on the server to support four simultaneous Fabric Manager sessions. The Management Server can either be a physical server, or a virtual machine within ESX infrastructure.

4.3. *Terminal Services License*

The Management Server must be licensed for Terminal Services because the server will be accessed via Remote Desktop by Storage Operations personnel. Please consult with your SA on how to obtain and deploy this license.

5. Management Server Build

Note: To completely uninstall the software for a fresh install, uninstall the SPAC and then manually remove the “C:\Program Files\Cisco Systems\MDS 9000” directory.

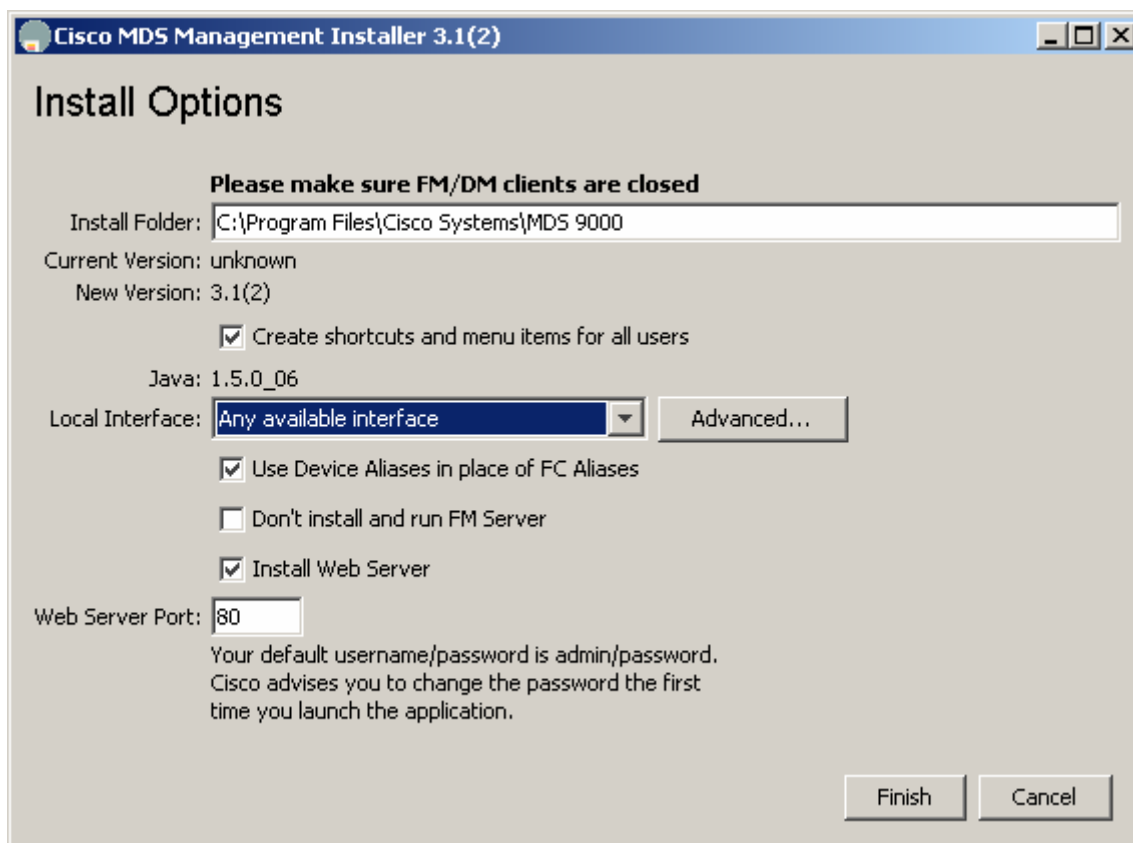
If you are planning to install Cisco MDS software on a server that runs other storage applications, please see appendix C: Resolving Application Conflicts for additional configuration steps.

5.1. *Step 1: Check for JRE*

Make sure Java Runtime Environment (“JRE”) version 1.5 or higher is available on the server. At the time of writing of this document, Java Development Kit v1.5.0_06 is available from GDSGOLD distribution server as SPAC ID “jks15060”. Please consult with your SA for the latest certified version of Java.

5.2. *Step 2: Install Fabric Manager*

Install SPAC ID “fbmg3110” from the GDSGOLD distribution server. Choose default install options.



5.3. Step 3: Secure Fabric Manager Server

Edit "C:\Program Files\Cisco Systems\MDS 9000\server.properties". Set "server.bindaddr=127.0.0.1".

5.4. Step 4: Secure Performance Manager Server

Edit C:\Program Files\Cisco Systems\MDS 9000\tomcat\conf\server.xml. In the "Connector" configuration, add "address=127.0.0.1" parameter. Do this for both HTTP and HTTPS connector definitions. It is not important where the address parameter appears in the configuration string.

This is what the "Connector" configuration should look like after making the changes (changes have been highlighted in **BOLD**):

```
<Connector className="org.apache.catalina.connector.http.HttpConnector"
    port="80" minProcessors="5" maxProcessors="75"
    enableLookups="false" redirectPort="8443" address="127.0.0.1"
    acceptCount="10" debug="0" connectionTimeout="60000"/>
<!-- Define an SSL HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.catalina.connector.http.HttpConnector"
    port="8443" minProcessors="5" maxProcessors="75"
```

```
enableLookups="true" address="127.0.0.1"  
acceptCount="10" debug="0" scheme="https" secure="true">  
<Factory className="org.apache.catalina.net.SSLServerSocketFactory"  
clientAuth="false" protocol="TLS"/>  
</Connector>
```

5.5. Step 5: Install SSH Client

Install Tectia Client 4.4.6.43 SPAC package ID tccl4420. This will install SSH client on the server.

5.6. Step 6: Install SFTP Server

Install Tectia Server 4.4.6.43 SPAC package ID tecs4421. This will install the SFTP server that can be accessed from the switch for exchanging firmware, configuration, script and license files.

Cancel the request to reboot the server. We will reboot once we are finished with other configuration.

5.7. Step 7: Configure FMS with Citi SSH

Fabric Manager allows you to right click on a device on the map to start a CLI session to the device. This is a very convenient feature. By default, Fabric Manager uses telnet but because telnet is disabled on the switch, SSH must be configured.

Log in to Fabric Manager Server as shown below. The default password is “password”.



Select a seed switch IP, username “admin”, and the password that was configured on the switch during switch configuration and click “Discover”.



Discover New Fabric - Fabric Manager

Seed Switch: 10.40.42.108

User Name: admin

Password: *****

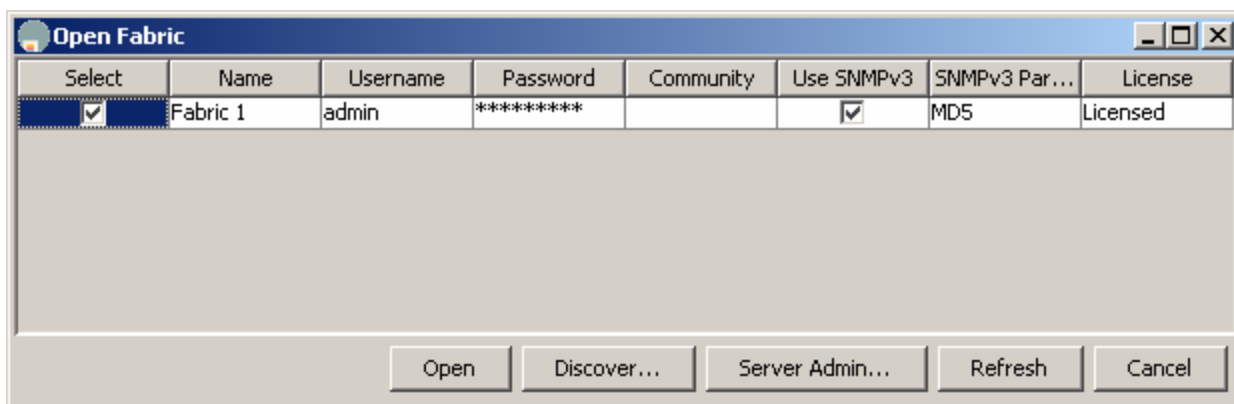
Use SNMPv3: ☒

Auth-Privacy: MD5

Accelerate Discovery ☒

Discover Close

Select any fabric and click “Open”.

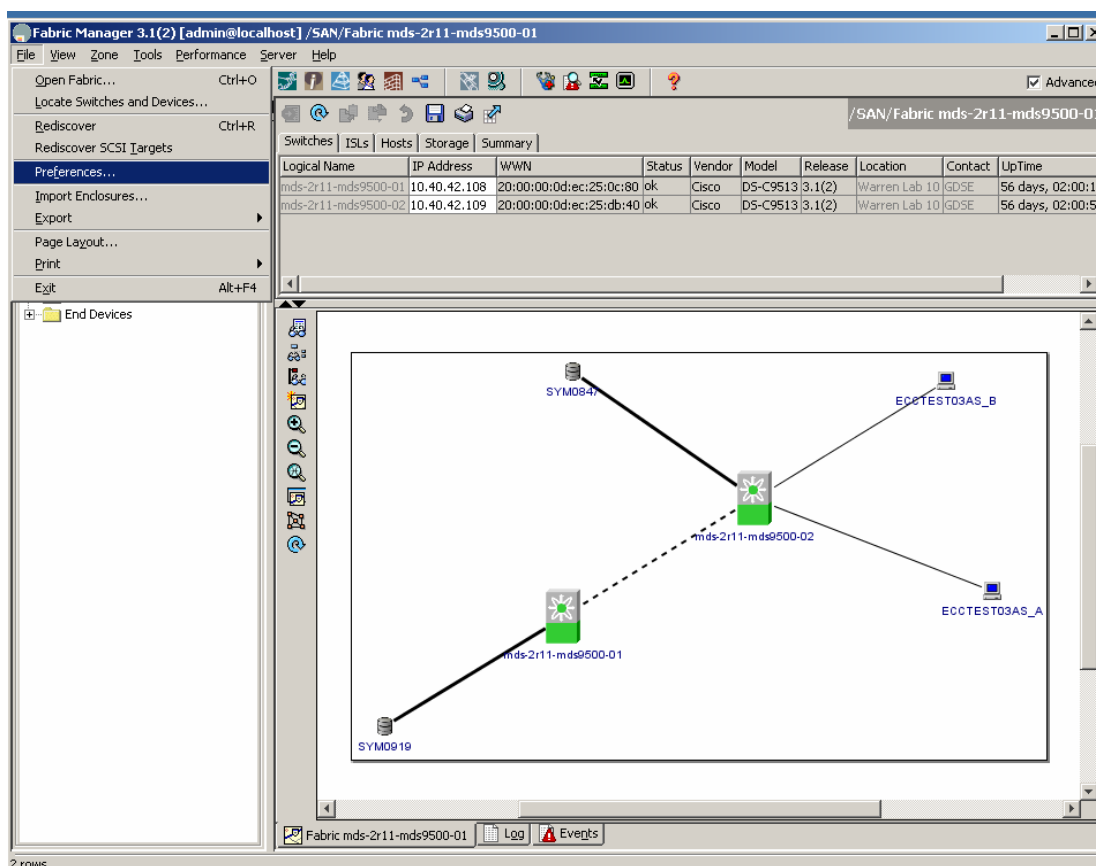


Open Fabric

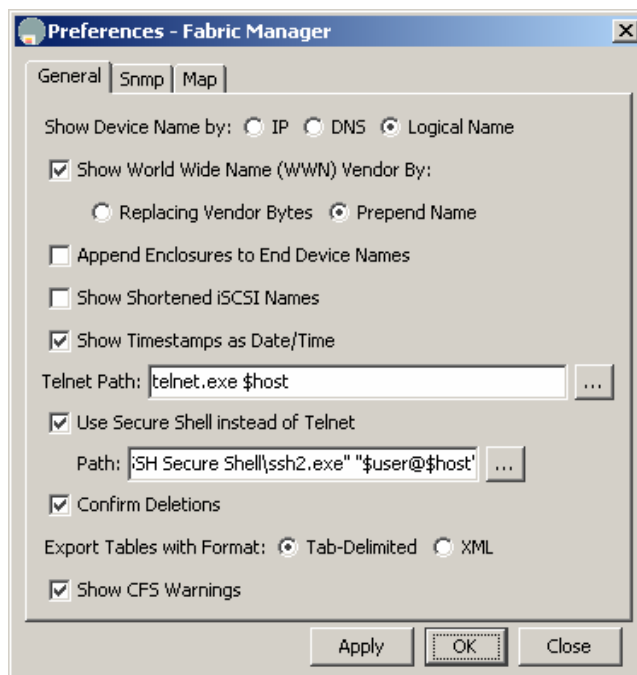
Select	Name	Username	Password	Community	Use SNMPv3	SNMPv3 Par...	License
☒	Fabric 1	admin	*****		☒	MD5	Licensed

Open Discover... Server Admin... Refresh Cancel

Click on File -> Preferences



Select "Use Secure Shell instead of Telnet" and for "Path" type the following:
`cmd /k start "$user @ $host" "c:\apps_srv\ssh\communications security\ssh secure shell\ssh2.exe" "$user@$host"`





If you prefer to use the Windowed version of SSH client instead of the command prompt version, configure the following “Path”:

```
"C:\apps_srv\SSH Communications Security\SSH Secure Shell\sshclient.exe" -u $user -h $host
```

Note: This configuration is stored in the user profile. As users are added to Fabric Manager, each user must follow the above procedure to enable SSH from the GUI.

5.8. Step 8: Configure Call-Home

5.8.1. Call-Home to EMC

When the MDS switches are supported by EMC, the Fabric Manager Server (FMS) should be configured to send fault alerts to EMC support center. FMS will be set up to relay email to a Citi mail relay server⁶.

Edit “C:\Program Files\Cisco Systems\MDS 9000\server.properties”. Customize the items in **red** with input from EMC:

```
# Enable or disable EMC Call Home. By default, it is disabled.
server.callhome.enable = true
```

```
# Specify Lab Location parameter.
server.callhome.location = street address of SAN site
```

```
# Specify 'From Email' list. The list should be comma seperated.
server.callhome.fromEmail = santeam@citi.com
```

```
# Specify 'recipientEmail' list. The list should be comma separated.
# [example. rnitur@cisco.com ]
server.callhome.recipientEmail = emcsupport@emc.com
```

```
# Specify the SMTP Host address for outbound email.
# [example. outbound.cisco.com ]
server.callhome.smtphost = Citi SMTP relay server. Obtain from Citi SMTP team.
```

Other settings such as site ID also need to be set up correctly. Please check with EMC personnel.

Restart the “Cisco MDS Fabric Manager” service from the Windows service control applet.

Note: For Call-Home to EMC to work, Fabric Manager must be configured to monitor fabrics continuously. GDSE recommends using the admin ID to monitor the fabrics. If at

⁶ By the end of Q4, 2007, GDSE would have certified MDS fault alerting (call-home) and remote access on ESRS for EMC supported MDS switches. ESRS will send alerts using HTTPS transport which is much more reliable and secure than email.



any time the password of the admin account is changed, the monitor continuously configuration must be repeated.

5.8.2. Call-Home to HDS

When the MDS switches are supported by HDS, the following configuration should be used to enable call-home to HDS support center. HDS provides free software called “Hi-Track” to monitor the Cisco MDS switches. This software uses read-only SNMP v1 to periodically run a health check on the switches being monitored. Fault reports are collected into a file and periodically sent to the HDS support center by using HTTPS transport. The support center reviews the fault report and tasks customer support engineers in the field.

Note: To completely uninstall Hi-Track for a fresh install, first uninstall the SPAC and then delete the “C:\HDS” folder with all sub-folders.

GDSE has certified version 3.9 of Hi-Track monitor. This software is available as SPAC ID hitr3910. Select all default options during the install.

Please have HDS support person assist you with this configuration. You will need several pieces of information from HDS before you can complete the configuration.

Browse to <http://127.0.0.1:6696> on the Management Server. Select “Administrator” user ID and password “hds” to logon.

Step a: Change the administrator password. The administrator account should be treated as a functional ID. The ID is only used to configure Hi-Track monitor. Because Hi-Track only has read-only access to the MDS switches it manages, this ID cannot be used to make any changes to the fabric and hence is a “read-only” functional ID.

Step b: Configure a new “User”. In detail for the user name, fill out “hitrack” for “Community String”

Step c: Configure a new “User”, “Proxy” called “CitiProxy”. In the “Detail” for the user name, fill in values for “Proxy Host” and “Proxy Port” the same as used by Internet Explorer on your desktop. For example, some North America desktops use “webproxy.ssmb.com” on port “8080” as the proxy.

Step d: Create a new “HTTPS” transport agent with the following detail:

Server: Please obtain from HDS. For NA the server name is ushtinet01.hds.com

Local Interface: -any-

Port: 443

UserName: Please obtain from HDS. For ushtinet01.hds.com server the user ID is “ht_http_row”

Password: Please obtain from HDS

Proxy ID: CitiProxy

Enabled: Yes

Step e: Add each Cisco MDS switch from the “Summary” menu to Hi-Track. While adding each switch, specify “hitrack” for the “SNMP Access ID”.

Step f: Configure each MDS switch: Create a read-only SNMP community string called “hitrack” for use by the Hi-Track monitor service. Please see Template.

Step g: Test Hi-Track: Make sure that the added devices are showing “Okay” status on the summary page. Now click on the “Request Report” button on the “Transport History” page. This will create report files that should be transported to the HDS server. After a few minutes, the transport history will show that the report files have been successfully transmitted to HDS.

5.9. Step 9: Configure FMS to authenticate to Active Directory

The Fabric Manager Server can authenticate users via RADIUS protocol to Microsoft Internet Authentication Service (“IAS”). IAS will accept user authentication requests from Fabric Manager and pass it on to Active Directory. Please see section 7.1 for step-by-step instructions on how to configure IAS and Active Directory. The following configuration should ONLY be done after those instructions have been executed.

Edit the following lines in the “C:\Program Files\Cisco Systems\MDS 9000\AAA.properties” file:

```
authentication.mode=radius
#Primary AAA server – IP address of the Management Server
aaa.server.primary.name=168.109.214.118
#Shared secret that you configured on IAS
aaa.server.primary.secret=cisco123
#Authentication method
aaa.server.primary.auth-method=PAP
```

Restart the “Cisco MDS Fabric Manager” service from the Windows service control applet. At this point only authorized users within Active Directory will be allowed to log on to the Fabric Manager and Performance Manager. The default userid “admin” and password “password” will not work.

In case IAS is down or incorrectly configured, you can reverse the entries in the aaa.properties file, restart the “Cisco MDS Fabric Manager” service and continue to use the “admin” user ID. Note that access to actual fabric and switch configuration is only granted after authentication to the switch which always goes to IAS/Active Directory.

5.10. Step 10: Management Server Access Control

Only authorized Citi storage and security management personnel should be authorized to log on to the Management Server. Please check with your SA on how to configure the server to support this. One way to accomplish this is to: (1) create a local group (2) assign this group the right to log on locally (3) add authorized storage administrators to this the group and (4) revoke the right to log on locally from all other groups and users.

5.11. Step 11: Reboot The Server

Reboot the server for the changes above to take effect.

6. Switch Configuration Steps

6.1. Step 1: Design VSAN IDs and Domain IDs

All ports are members of the default VSA, VSAN 1. GDSE recommends that Port Security should not be turned on for VSAN 1. This would allow facility personnel to cable up hosts and storage to the switch and verify fabric logon. Afterwards, Storage Administrator would move the port to a production VSAN where Port Security is enabled.

It is important to design VSAN ID as and Domain IDs in such a way that future applications such as migrations between VSANs (fabrics) can be supported without significant configuration change. The goal is to try to avoid using AFID and NAT with IVR, and the simplest way to achieve that is to keep VSAN IDs and Domain IDs unique across the region. However this is not practical for large regions such as North America because there are only 239 domain IDs.

Problem	Cisco's Solution	Challenges with Solution
Overlapping VSAN IDs	Autonomous Fabric ID (AFID)	Reduces total number of VSANs allowed in the fabric (not a show stopper); additional configuration required
Overlapping Domain IDs	Network Address Translation (NAT)	Introduces limitations (no showstoppers); additional configuration required

It should be noted that IVR will only be used for migration between VSANs, not for BAU provisioning and replication tasks. Host to storage connections, as well as replicating end points should be members of the same VSAN.

Because the frequency of migrations within datacenter would be much higher than across datacenters **unique domain IDs should be maintained within each datacenter**. Also, because VSAN IDs provide a large range, 2 – 4093, **VSAN IDs should be unique across a region**.

Domain IDs are managed per VSAN. The IDs you reserve or assign to a switch for one VSAN has no bearing on other VSANs hosted by the switch.

Because there are only 239 domain IDs, domain IDs should be conserved. Because Fabric A and Fabric B will never be connected via IVR, **same domain IDs should be used for these fabrics**.

Further, to keep things simple, each switch should be allocated the **same domain ID for every fabric**.

Blocks of domain IDs should be reserved for each VSAN (fabric) within the datacenter. Because the largest fabric (see fabric design section in this document) can have 12 switches, **a block of 12 domain IDs should be reserved for each fabric**.

The **MDS allows you to configure the reserved range of domain IDs per fabric**. This configuration will prevent an Operator from mistakenly assigning a domain ID outside the reserved range to a newly added switch. This configuration has been included in the Template.

Fabric A and Fabric B should be assigned different VSAN IDs. This will add another layer of protection when A and B fabrics are inadvertently merged. A range of **even numbered IDs should be reserved for Fabric A, and odd numbered IDs for fabric B per SAN**. **GDSE recommends reserving 6 VSAN IDs per fabric**, which will permit 682 fabrics or 341 total SANs in the region that can be interconnected with IVR without using AFID. **VSAN IDs 4002-4093 should not be used**; these should be reserved for transit VSANs for use with IVR.

Sample allocation of VSAN and Domain IDs:

SAN 1, Datacenter 1

VSAN IDs	VSAN Name	Reserved Domain IDs
1	Default	Don't care
2	Fabric A	1-12
3	Fabric B	1-12
4,6,8,10,12	Additional 'A' fabrics for future use	1-12
5,7,9,11,13	Additional 'B' fabrics for future use	1-12

SAN 2, Datacenter 1

VSAN ID	VSAN Name	Domain IDs
1	Default	Don't care
14	Fabric A	13-24
15	Fabric B	13-24
16,18,20,22,24	Additional 'A' fabrics for future use	13-24
17,19,21,23,25	Additional 'B' fabrics for future use	13-24

SAN 1, Datacenter 2

VSAN ID	VSAN Name	Domain IDs
1	Default	Don't care
26	Fabric A	1-12
27	Fabric B	1-12
28,30,32,34,36	Additional 'A' fabrics for future use	1-12
29,31,33,35,37	Additional 'B' fabrics for future use	1-12

SAN 2, Datacenter 2

VSAN ID	VSAN Name	Domain IDs
1	Default	Don't care
38	Fabric A	13-24
39	Fabric B	13-24
40,42,44,46,48	Additional 'A' fabrics for future use	13-24
41,43,45,47,49	Additional 'B' fabrics for future use	13-24

Because VSAN 1 will not be used for production, and because there will not be any IVR application for VSAN 1 in the future, there is no need to plan for domain IDs for VSAN 1. Domain IDs for VSAN 1 will be assigned dynamically by the principle switch.

6.2. Step 2: Design Naming

Switch names	Max length is 32 characters, must start with a letter, not supported ~ ! @ # % & * () = + [] { } \ ; ' : " , . / < > ?
VSAN names	Max length is 32 characters, No special character limit
Zone names	Max length is 64 characters, must start with a letter, not supported ~ ! @ # % & * () = + [] { } \ ; ' : " , . / < > ?
Zoneset names	Max length is 64 characters, must start with a letter, not supported ~ ` ! @ # % & * () = + [] { } \ ; ' : " , . / < > ?
Device Alias names	Max length is 64 characters, must start with a letter, not supported ~ ` ! @ # % & * () = + [] { } \ ; ' : " , . / < > ?

Device alias and not FC alias names should be used for zoning. To make it easy to track a logged out HBA to a switch port, the device alias may include the switch name and port number, unless such information is being tracked in another system such as a spreadsheet or SANScreen.

To prevent inadvertent interconnection of Fabric A and Fabric B, port channels in Fabric A should be even numbered and in Fabric B should be odd numbered.

6.3. Step 3: Customize Configuration Template

Copy the Configuration Template from appendix D into a Wordpad document on the Management Server. Edit the text marked in red to suit the specific switch and site that is being configured. Save the file as a text file in the user's home directory: if the userID logged on to the Management Server is "user123" then the home directory is "C:\Documents and Settings\user123". Use a short file name without spaces to make the copy to switch process simpler. This file is the "Configuration Script".

6.4. Step 4: Power Up and First Login

Connect the two console connections and configure the terminal server to operate the lines at 9600 baud, 8 databits, 1 stop bit and no parity. Use telnet to terminal server and connect to the

console port on the supervisor in the lower numbered slot (the supervisor in the lower numbered slot will become the active supervisor). Power up the switch. When prompted, configure a new CISS complaint password for the “admin” user, and enter “no” when asked “Would you like to enter the basic configuration dialog (yes/no)”. Now logon as “admin”.

6.5. Step 5: Configure IP Address & Default Gateway

Configure IP address, subnet mask and default gateway by issuing the following commands. Replace the text in red with your own addresses.

```
conf
interface mgmt0
  switchport speed 100
  ip address 10.40.42.108 255.255.255.0
exit
ip default-gateway 10.40.42.2
exit
```

6.6. Step 6: Upgrade SANOS to GDSE Certified Version

The following command will show the SANOS version:

```
Switch# show version
```

Using your Cisco Connection Online (“CCO”) account, or with help from vendor support, download the correct System and Kickstart SANOS images from Cisco’s website to your home directory⁷ on the Management Server. Now copy both files to switch bootflash filesystem using the following command on the switch:

```
Switch# copy sftp://MgmtServerIP/homeSystemImageFileName bootflash:SystemImageFileName
```

```
Switch# copy sftp://MgmtServerIP/home/KickStartImageFileName
bootflash:KickStartImageFileName
```

Start the upgrade (or downgrade) process with this command:

```
Switch# install all system bootflash:SystemImageFileName kickstart
bootflash:KickStartImageFileName
```

The system will be now be upgraded (or downgraded). Please note that there is a Supervisor switchover during the upgrade so you will have to connect to the console of the other Supervisor to carry out rest of the configuration.

⁷ This is the directory that the Tectia server makes accessible via SFTP. If you are logged in to the Management Server as “im12345” SOE ID, the home directory is “C:\Documents and Settings\im12345”.

6.7. Step 7: Copy Configuration Script from Step 3 to Switch Filesystem

```
copy sftp://MgmtServerIP/home/scriptFileName bootflash:scriptFileName
```

6.8. Step 8: Run the Configuration Script

```
run-script bootflash:scriptFileName
```

If there are errors reported at the end, “write erase” and “reload” the switch and start over from step 1, making sure that errors in the script are fixed.

6.9. Step 9: Obtain and Install Licensing

The following licenses are required to be installed:

```
FM_SERVER_PKG  
ENTERPRISE_PKG
```

If you are going to use SAN Extension over IP (FCIP), you will need additional licenses for that. Please refer to the FCIP Solutions Guide available from <http://engineering.citigroup.net/gdse/products/platforms/ciscomds/?a=5441>

The MDS has a “feature” that allows for unlicensed features to be used normally. The switch does this by turning on the demonstration mode that expires after a certain period, usually 120 days⁸, from the date the feature was first used⁹. The features will automatically get disabled after expiry of the demonstration license, and can cause an outage. Operations must make sure that all required licenses have been deployed to the switch before declaring it operational. **Making the switch operational first and deploying licenses later is NOT a good practice; it can lead to a major outage.**

Steps to obtain and install licenses:

- Browse to <http://cisco.com> and register to obtain a Cisco Connection Online (“CCO”) user ID
- Browse to <http://cisco.com/go/license>
- Enter the Product Activation Key (“PAK”) that came with the product
- Obtain serial number of switch where license needs to be installed with:

```
Switch# show license host-id  
License hostid: VDH=FOX100606TD
```

Ignore the “VDH=”; the remaining string (highlighted above) is the serial number.
- Enter the serial number

⁸ The length of the demonstration period cannot be extended by setting back the date on the switch

⁹ GDSE has requested Cisco to discontinue this feature in future SANOS releases

- Make sure to check your email address in the displayed user profile because keys are sent by email
- Submit the request
- Within a few minutes you will see an email with a .lic file attachment. This is the license file.
- Copy the .lic file to your home directory on the Management Server. Copy and install the .lic file to the switch bootflash:

```
Switch#copy sftp://MgmtServerIP/home/licenseFileName bootflash:licenseFileName
Switch# install license bootflash:licenseFileName
```

The following output shows that the required licenses have been correctly installed.

```
Switch# show license usage
```

Feature	Ins	Lic Count	Status	Expiry Date	Comments
FM_SERVER_PKG	Yes	1	In use	never	-
MAINFRAME_PKG	No	0	Unused		-
ENTERPRISE_PKG	Yes	1	In use	never	-
SAN_EXTN_OVER_IP	No	0	Unused		-
PORT_ACTIVATION_PKG	No	0	Unused		-
SAN_EXTN_OVER_IP_18_4	No	0	Unused		-
SAN_EXTN_OVER_IP_IPS2	No	0	unused		-
SAN_EXTN_OVER_IP_IPS4	No	0	Unused		-
10G_PORT_ACTIVATION_PKG	No	0	Unused		-
STORAGE_SERVICES_ENABLER_PKG	No	0	Unused		-

7. User IDs and Authentication

7.1. Interactive Authentication

Although the switch and Fabric Manager can host user IDs, it is advisable to authenticate users from an external system to follow the principle of separation of duties. External authentication system will also generally provide more compliant authentication by enforcing password complexity, password expiration, and user account expiration.

The Citi standard for authentication of users to hardware devices such as Cisco network devices is Cisco Access Control Server (“ACS”). Currently ACS is used for authentication of all Cisco Ethernet and IP devices globally. However, although the MDS switch and Fabric Manager support the TACACS+ protocol, they do not additionally support the “ENIGMA” protocol, which is required by Citi’s implementation of ACS. ENIGMA permits relaying of authentication requests from the device to Safeword systems via ACS. This relaying is required because the authentication built into ACS is not fully complaint with CISS.

The solution outlined here will thus not use ACS, but rather use Windows Internet Authentication Service (“IAS”) to relay authentication requests from switch and Fabric Manager to Active Directory. All user add, delete, modify, as well as entitlement operations, will occur within Active Directory. The benefits of this approach over local user IDs are:

- Because authentication is delegated to Active Directory, there will be full compliance with CISS authentication standards
- Users can use their SOEID to log on; MASTER ID compliance is automatically achieved
- There is separation of duties: Storage Operations will not control user IDs and entitlements
- Management of user IDs will be centralized

IAS is a component of the Windows 2003 Server operating system. No additional license is required to use IAS. The Citi Windows 2003 Server build process does not install IAS. It must be manually installed after the build is completed. Here is an overview of the installation and configuration process:

- ✓ Ask for Active Directory groups to be created
- ✓ Install and configure IAS on the Management Server
- ✓ Configure switches
- ✓ Configure Fabric Manager

Here are detailed step-by-step instructions to accomplish the above.

Step1: Create and Populate Active Directory Security Groups

Ask your Active Directory administrator to create following Active Directory security groups. The Active Directory group names are only suggestions; the Active Directory administrator should formulate the names based on Active Directory conventions. Any existing groups can also be used instead of getting new ones created specifically for MDS.

Active Directory Security Group	Purpose: Maps to this role on the switch	Members
MDS_Storage_Admin	storage_admin	Storage Operations personnel
MDS_Network_Admin	network-admin	Select Storage Operations personnel
MDS_Vendor	vendor	“emc” and “hds” functional IDs ¹⁰
MDS_Facility	facility	Facility Operations personnel who will hook up hosts and storage to MDS

The following steps require Administrator rights on the Management Server.

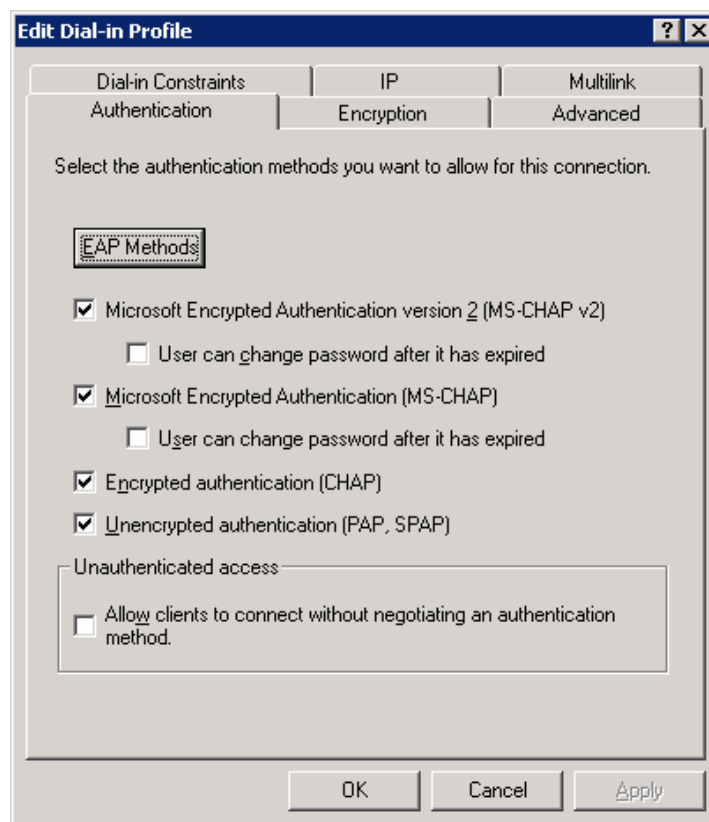
¹⁰ Please contact your BISO for instructions on how to get functional IDs approved and created. If it is not possible to have these functional IDs created on Active Directory, these should be created as local Windows IDs on the Management Server.

Step 2: Install Windows Internet Authentication Service ("IAS") on the Management Server

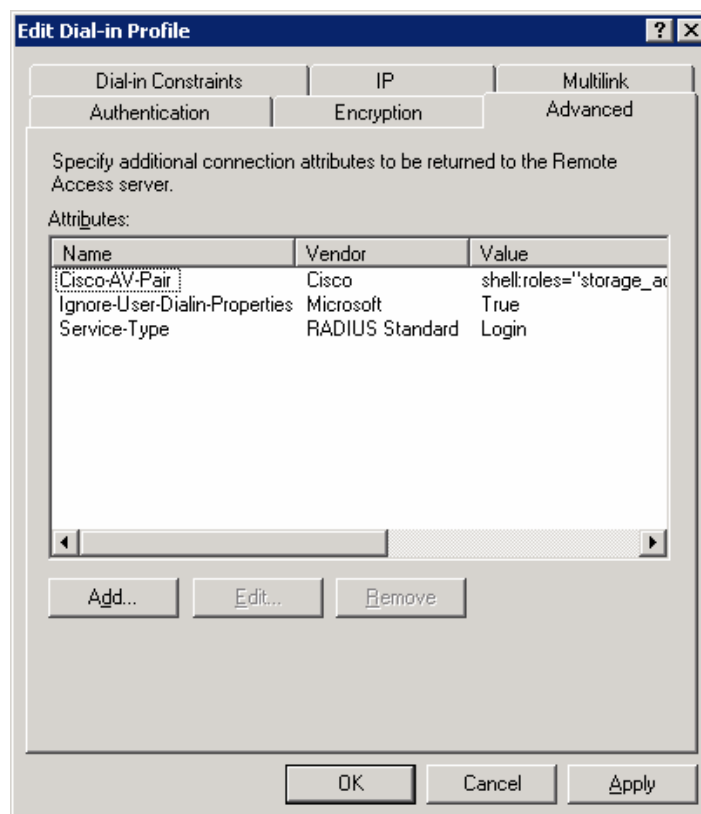
From Control Panel, Add/Remove Programs, Add/Remove Windows Components, click on "Networking Services" and click on Details. Select "Internet Authentication Service". Make sure none of the other services are selected. Click OK. Click Next. IAS will now be installed.

Step 3: Configure IAS: Create Policies

- From Start Menu, select Programs, Administrative Tools and click on Internet Authentication Service.
- Click on Remote Access Policies
- Delete all existing policies visible in the right pane
- Right click on Remote Access Policies and click on New Remote Access Policy
- Click Next
- Select Set up a custom policy
- For Policy name, enter "MDS Storage Admin"
- Click Next
- Click Add
- Select Windows-Groups and click Add
- Click Add
- Enter the Active Directory group name for Storage Administrators that you created in Step 1. For example: NAM\MDS_Storage_Admin. You may be asked to provide a user account in the domain where this group resides so that the group name can be validated. Any user account (domain administrator account is not required) can be provided.
- The group should now be listed in the Groups list. Click OK
- Click Next
- Select Grant remote access permission and click Next
- Click Edit Profile
- Configure the Authentication as following:

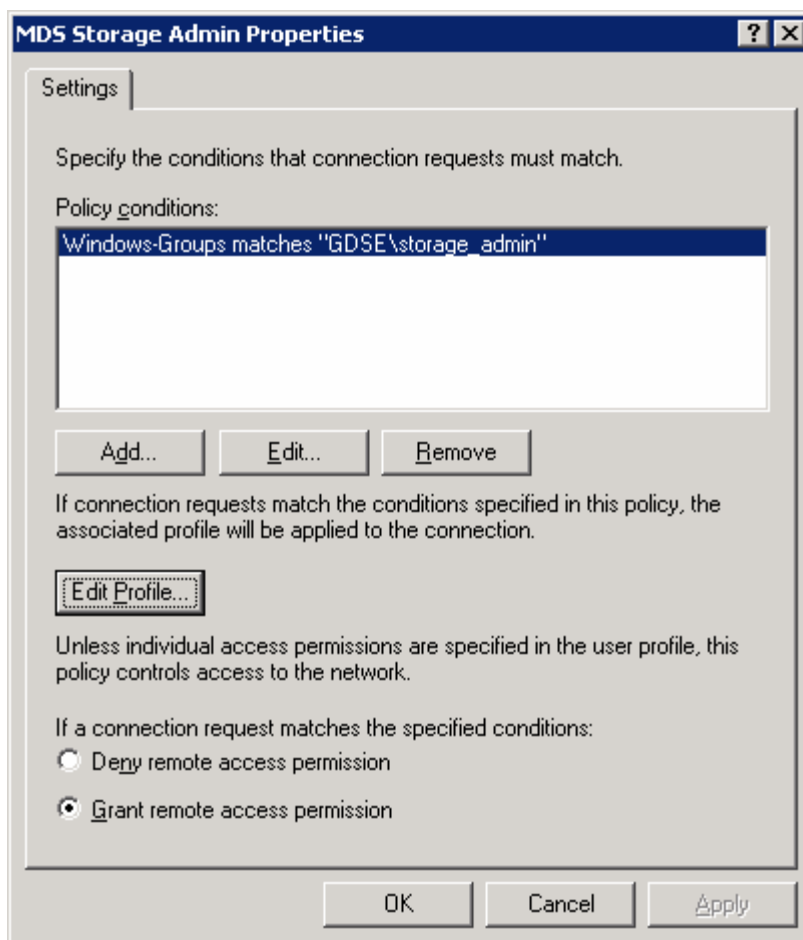


- Configure Advanced as following:



The Cisco-AV-Pair value in the above screenshot is *shell:roles="storage_admin"*. The string within quotes, "storage_admin" must exactly match the role name defined on the switch.

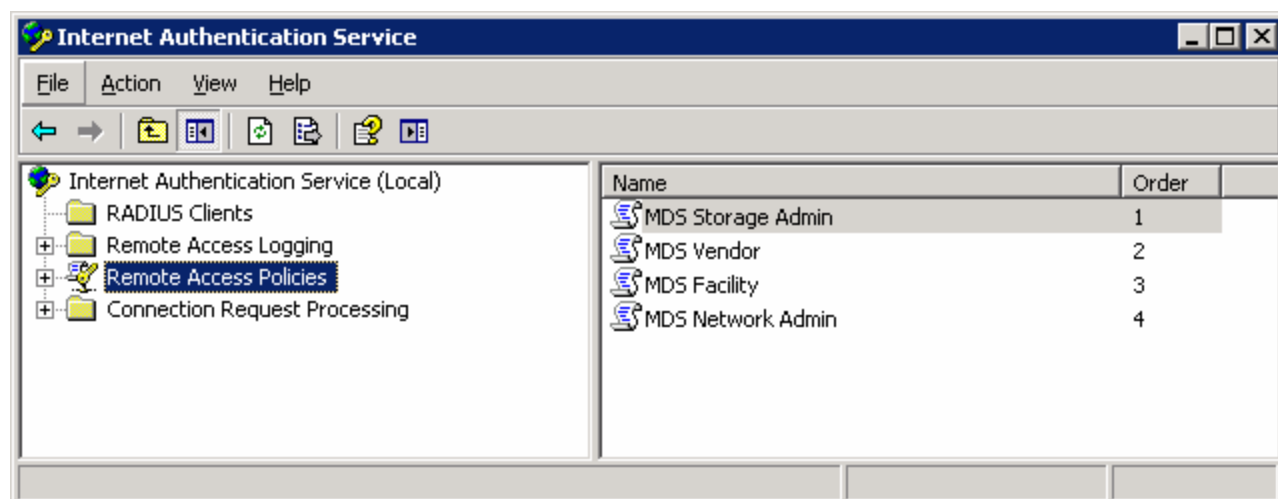
- Click OK. The completed policy should look like this:



- Click OK.
- Create three more policies, one for each group defined on the switch:

Policy Name	Active Directory Group	CISCO-AV-PAIR
MDS Storage Admin	MDS_Storage_Admin	shell:roles="storage_admin"
MDS Vendor	MDS_Vendor	shell:roles="vendor"
MDS Facility	MDS_Facility	shell:roles="facility"
MDS Network Admin	MDS_Network_Admin	shell:roles="network-admin"

With all four policies created, this is what the IAS main screen should look like:



Step 3: Configure IAS: Add Clients

Each MDS switch and Fabric Manager Server (Management Server) has to be added as a client.

- Right click on RADIUS Clients and click on New Radius Client
- Enter the switch/server name for Friendly name
- Enter the IP Address of the switch/server
- Click Next
- For Client-Vendor select RADIUS Standard (this is selected by default)
- Enter a shared secret for the client. This is an arbitrary string without spaces. Make a note of the secret because you will have to configure the same secret on the switch/server.
- Do NOT check "Request must contain the Message Authenticator attribute"
- Click Finish

Repeat the above procedure for all switches and Management Servers.

Step 4: Configure Fabric Manager

Please see section 5.9

Step 5: Configure Switch

Please see the configuration template in appendix D. Search for “Authenticate to IAS via RADIUS” section.

The authentication configuration is now complete.

7.2. Purpose of Network-Admin Role

The default “admin” user ID on the switch is a member of the Network-Admin role, which has full privileges on the switch. This ID cannot be deleted. The password for “admin” should be

stored in a safe place. Some select Storage Operations personnel should also be made members of the Active Directory group that corresponds to the network-admin group.

These IDs should not be used for BAU tasks, but for the following exceptional situations:

- IAS/Active Directory is down or incorrectly configured and you are unable to log on. In this case you can use the “admin” ID to log on via the console port and reset the configuration
- The management interface is not accessible due to:
 - o Bad IP ACL entry
 - o Incorrect IP address, mask or default gateway
 - o The physical Ethernet interface has failed

In such cases the switch can be accessed via the console port by using the “admin” ID.

- Existing role definitions need to be modified. A user with network-admin privileges can make these changes.
- New roles need to be added. A user with network-admin privileges can add new roles.
- Non-interactive authentication users (see following section) need to be created locally on the switch. A user with network-admin privileges can create such users.

7.3. Non-Interactive Authentication

Scripts that do not alter switch configuration, such as those that will report user entitlements or backup switch configuration, can use non-interactive, public/private key based authentication. Scripts that will make changes to the configuration, should be started and monitored by an Operator and therefore should continue to use interactive authentication. Under no circumstances should usernames and passwords be coded in the script.

One or more user accounts can be created for scripts that will use public/private key based authentication. From a security assessment perspective, these user accounts will be treated as functional IDs with read only privileges. The following illustrates how the key pair can be generated and associated with a user account on the switch.

Note: Throughout the following discussion it will be assumed that user ID “im12345” is logged on to the Management Server. Paths will change if a different user is logged on.

Step1: Generate keys by using SSH utilities on the Management Server

```
ssh-keygen2 -t rsa -P key
```

This will generate two files under the “c:\documents and settings\im12345\application data\ssh\userkeys:

key: file containing private key

key.pub: file containing public key

Step 2: Copy the public key file to the switch bootflash: by using SFTP from the switch

You will need to copy the key.pub file to the user’s home directory to be able to access it from sftp on the switch. The home directory for user “im12345” is “c:\documents and settings\im12345”.

```
Switch# copy sftp://MgmtSvrIP/home/key.pub bootflash:key.pub
```

Step 3: Associate the public key with a user account on the switch

! Enter configuration mode
config

! Create a new user called scriptuser
username scriptuser

! Associate the public key just copied to this user
username scriptuser sshkey file bootflash:key.pub

! Do not forget to give limited privileges to this user
username scriptuser role script¹¹

! Exit config mode
exit

! Delete the public key file
delete bootflash:key.pub

! Save
copy run start

Step 4: Test the account by logging on to the switch

```
ssh2 scriptuser@switch.citi.com
```

You should be logged in without being asked for a user ID or password.

Use the -v switch with ssh2 command line to troubleshoot any problems.

¹¹ Please see Template for a definition of the role “script”

8. Audit Trail Management

The MDS switch captures all security and system administration events in an internal log that can be accessed through CLI or Device Manager. The switch is also capable of sending these events to external system(s) via the SYSLOG protocol as they occur. GDSE's recommendation is to use a SYSLOG server to collect the events from the switch into a text file on the server, and then use eTrust Audit agent to scoop events from the text file and send it to eTrust Audit repository for further processing, archiving and reporting¹².

All possible messages that the MDS can produce are documented in this guide:

http://www.cisco.com/en/US/products/ps5989/products_system_message_guide_book09186a00804194b8.html

Audit logs should be periodically reviewed by the Storage Operations team to meet the following objectives:

1. Identify and investigate attempts to gain unauthorized access to the switch
2. Reconcile changes
3. Investigate root cause of a security incidence (forensic analysis)

Example: The SYSLOG server on a SOE Solaris server can be used to gather log events from the MDS:

Step 1: Configure the Solaris Server

Add the following line in the `/etc/syslog.conf` file:

```
local1.debug                                /var/adm/MDS_messages
```

There must be exactly 5 TAB characters between “local.debug” and “/var/adm/MDS_messages” strings. You may choose any other filename and location for the message file. After making the change, the syslogd daemon must be restarted for changes to take effect. Any audit events from one or more MDS switches will now be recorded into the “/var/adm/MDS_messages” file.

Step 2: Configure the Switch

See switch configuration template in appendix D.

In order for the date and time stamp on the log events to be accurate and consistent with other systems, the switch should be configured to synchronize its clock with one or more Citi NTP servers. NTP servers in every region are listed here

¹² If eTrust Audit is not yet available in your region, you should get an ETA for when it will be available, and create a PCM to review audit logs on the SYSLOG server itself.

http://www.Citi.net/tie/neteng/core/ntp/GNAST-ENG-0014_Network_Timing_Protocol.doc

See Template for NTP server configuration on the switch.

Integration with eTrust Audit will be discussed in a separate section in this document.

9. Vendor Remote Access

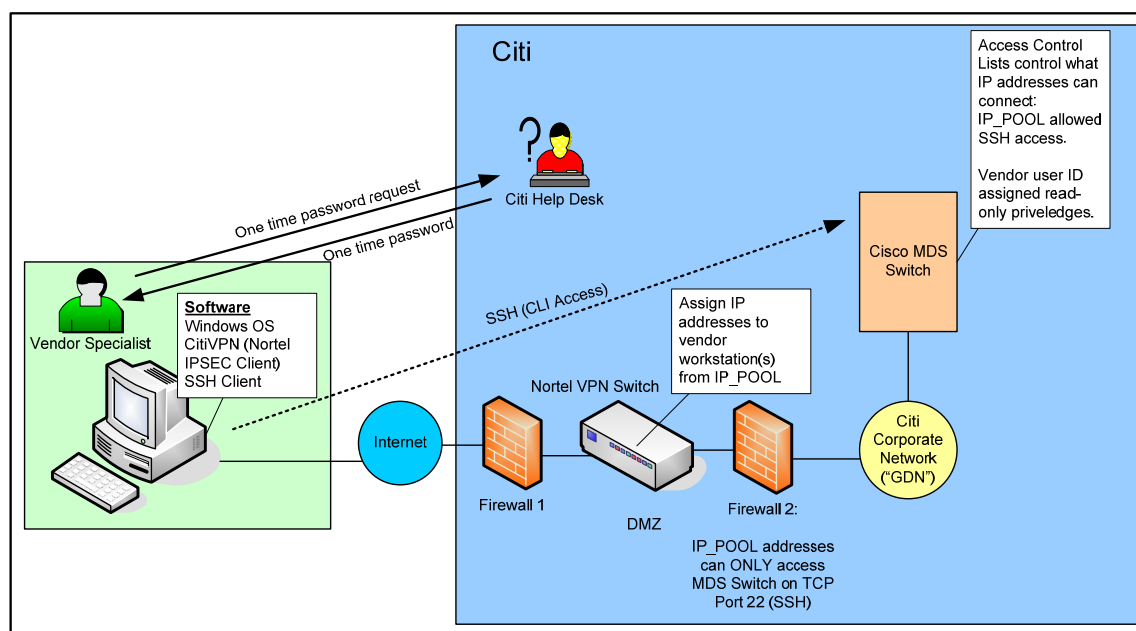
Vendor Remote Access will be provided so that vendor specialists can remotely log in to the MDS switch to quickly troubleshoot any problems.

Both EMC and HDS are working on a solution to provide remote support for the MDS. EMC is going to include support for MDS in their EMC Secure Remote Support Gateway (“ESRS”) product by the end of Q4 2007. ESRS has already been certified by GDSE for remote support of other EMC products such as Symmetrix. HDS is working on their SSL tunnel type solution with ETA of Q1 2008.

Until these solutions becoming available from the vendors, GDSE has created a tactical solution for remote access to the MDS switch. Both EMC and HDS have tested this access method and approved it. Vendor customer support specialists will use a Windows workstation and either a telephone line (DialVPN) or Internet connection (CitiVPN) to connect to Citi:

<http://engineering.citigroup.net/extsvcs/products/virtualprvatenetwork/?a=5441>

For any questions regarding the CitiVPN or DialVPN products or configuration, please contact product owner James T Wong, james.t.wong@citi.com or *GT US Authentication.



Requesting CitiVPN for MDS is a three step process¹³:

Step 1: A C3PAR connection entity should be created and approved

Step 2: Existing HDS/EMC safeword IDs that are currently being used for WWDS access to storage arrays or Connectrix products must be associated with "VPN ACL 144". For this, the existing sponsor of the safeword IDs must open a Virtual Security Request ("VSR"). Please note that EMC safeword IDs are different than HDS safeword IDs. Because we will be deploying switches supported by EMC or HDS, it is recommended that ALL safeword IDs (EMC and HDS) should be added to VPN ACL 144.

Step 3: Once the IDs have been associated with VPN ACL 144, an "IP Registration Request" should be submitted; please fill out

http://remoteaccess.Citi.net/files/Documents/ACL/ip_v1.3.doc

and HAVE YOUR BISO send it to "*GT US Authentication". You need to fill out the following:

Section A:

Contact details of the vendor. Use the name registered on CASP: For EMC use "EMC" for HDS use "Hitachi Data Systems"

UIC/SOEID (if known): Leave blank

¹³ These steps may vary from region to region. Please work with your BISO, ISA and Remote Access teams to discover the process followed in your region.

ACL (if known): VPN ACL 144

AP: leave blank

Section B:

Contact details of the Storage Operations person sponsoring the remote access

Section C:

Contact details of the Storage Operations BISO

Section D:

Contact details of the Storage Operations person sponsoring the remote access

Connection Type: PPP

Business Type: Production

Access Type: VPN

Business Reason for request: Remote support

Application Function: Fibre Channel (SAN) Switch

The table should list all MDS switches:

Host Application: SSH server

IP Address: IP address of the switch

DNS Name: DNS name of the switch

Ports: TCP/22 (SSH)

A: Port purpose: Console (command prompt) access for diagnostics and troubleshooting the switch

B: Compensating Controls: Only select commands are being enabled for the user at the command prompt

C: Comments: The Cisco MDS switch is a fibre channel switching device used to build Storage Area Network (SAN). High availability of this switch is critical and therefore there is a provision for vendor specialists to remotely log on to the switch for direct access to information to aid diagnostics.

10. Integration with ECC

EMC Control Center (“ECC”) is Citi standard SAN monitoring, reporting and provisioning software application. Please see

<http://engineering.citigroup.net/gdse/products/services/ecc/?a=5441>.

Currently, only storage utilization reporting capabilities of ECC have been certified by GDSE. As such, there is no need to integrate the MDS with ECC at this time. Future releases of ECC from GDSE might require integration that will be addressed as a part of the ECC project.

11. Integration with SanScreen

SanScreen from Onaro is the Citi standard change monitoring and planning tool for SANs. Please see

<http://engineering.citigroup.net/gdse/products/services/sanscreen/?a=5441>

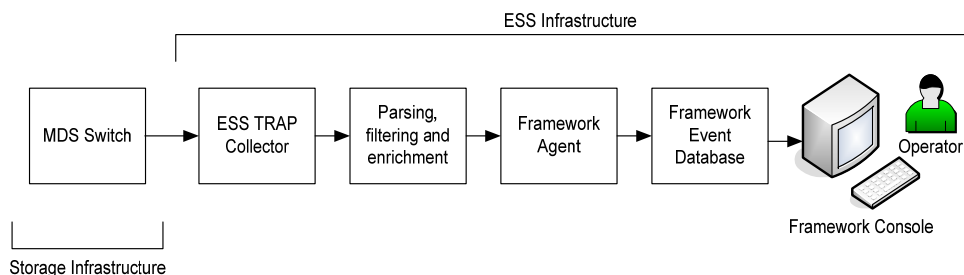
MDS was successfully tested with SanScreen version 3.5.2.8. This version or higher is required for successful integration with MDS; GDSE tested with version 3.0 and found show stoppers such as not all zones and VSANs being reported.

A read-only SNMP v1 community string must be created on all MDS switches that need to be monitored by SanScreen. Please see Template.

The Access Control List on the switch must be also modified to allow SNMP access from the server running SanScreen Acquisition Unit. Please see Template.

12. Monitoring the Switch with ESS

The MDS switch should be monitored by Enterprise Systems Services (“ESS”). The switch will generate SNMP v1 TRAPS for select events, such as power supply failure, link failure, etc. The TRAPs will be received by an ESS TRAP collector server and the events posted to a text file. A script will then parse and filter the events.



The framework agent will then gather the processed events and report these to the console. The console will be monitored 24x7 by the Console Operator(s). A Process Control Manual (“PCM”) developed by Regional Storage Operations teams will direct the Console Operator to deal with alerts that show up on the console. Another PCM developed by Regional Storage Operations team will direct Storage Operator actions against all possible events.

12.1. Implementation Steps

- ✓ Storage Operations team will engage regional ESS engineering/integration teams:

Region	Framework	Owner
APPC	BMC Patrol	Jit-Soon Koh
Mexico	HP Openview, MOM	Alfonso Diaz Jimenez
EMEA	Tivoli, Ice	Sean Lonegran
Japan	Tivoli, Ice	Carl Pickin
NA	Tivoli, Ice, NetIQ, MOM, HP Openview	Roger Kutchaver

- ✓ Regional ESS engineering/integration team will:
 - o Configure the TRAP collector server(s)
 - o Create scripts to parse, filter, enrich and categorize TRAPS according to GDSE specifications contained in the following section
- ✓ Storage Operations will configure the Cisco MDS switches
- ✓ Storage Operations will test the system by triggering test TRAPS from MDS

12.2. TRAPS to Monitor

All the MIBs supported by Cisco MDS SAN-OS 3.x software are in this file:

http://www.cisco.com/application/x-zip-compressed/en/us/guest/products/ps6030/c1225/ccmigration_09186a0080797145.zip

Cisco also provides an online MIB browser tool at:

<http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en>

GDSE has identified the following TRAPS for use within Citi:

Color Code	Category
	Critical
	Warning
	Informational

Enterprise ID of TRAP	Specific Type	Category	Description	Generate alert only if variable	Include in the Message ¹⁴	Variable Type
1.3.6.1.4.1.9.9.276	1		Link Down	N/A	Interface Name = 1.3.6.1.2.1.31.1.1.1.1	String
1.3.6.1.4.1.9.9.289.1.3	1		(E)ISL Port Down	1.3.6.1.4.1.9.9.289.1.1.3.1.1.* = 2 (down)	Cause = 1.3.6.1.4.1.9.9.289.1.1.3.1.3.*	String

¹⁴ All messages should include the IP address and/or the DNS name of the switch sending the TRAP and the Description

Enterprise ID of TRAP	Specific Type	Category	Description	Generate alert only if variable	Include in the Message ¹⁴	Variable Type
1.3.6.1.4.1.9.9.282.1.3	1		VSAN Status Change to DOWN	1.3.6.1.4.1.9.9.282.1.1.3.1.8.* = 2 (down)	VSAN ID = 1.3.6.1.4.1.9.9.282.1.1.4.*	Positive Integer, range 0 – 4096
1.3.6.1.4.1.9.9.302.1.3	3		Build Fabric (BF) or ReConfigure Fabric (RCF) Event	N/A	VSAN ID = 1.3.6.1.4.1.9.9.282.1.1.4.*	Positive Integer, range 0 – 4096
1.3.6.1.4.1.9.9.294.1.4	2		Zone Merge Failure	N/A	VSAN ID = 1.3.6.1.4.1.9.9.294.1.3.3.*	Positive Integer, range 0 – 4096
					Failure Reason = 1.3.6.1.4.1.9.9.294.1.3.6.*	1:other 2:zoningModeMismatch 3:qosNotEnabled 4:qosConflict 5:bcastNotEnabled 6:mergeCtrlMismatch 7:defZoneMismatch 8:qosAttrMissing 9:bcastAttrMissing 10:rdonlyAttrMissing 11:memberMismatch 12:invPayloadFormat 13:sizeExceeded 14:unlicensedMember 15:nonInteropZoneset
1.3.6.1.4.1.9.9.91.2	1		Temperature exceeded threshold	N/A	Threshold temperature = 1.3.6.1.4.1.9.9.91.1.2.1.1.4.*	Positive Integer range 0-200
					Current Temperature = 1.3.6.1.4.1.9.9.91.1.1.1.1.4.*	Positive Integer range 0-200
1.3.6.1.4.1.9.9.117.2	6		Fan Tray Status	1.3.6.1.4.1.9.9.117.1.4.1.1.1.* ≠ 2	Fan tray status = 1.3.6.1.4.1.9.9.117.1.4.1.1.1.*	1 : unknown 2 : up 3 : down 4 : warning
1.3.6.1.4.1.9.9.117.2	2		Power Status	1.3.6.1.4.1.9.9.117.1.1.2.1.2.* ≠ 2	Power status = 1.3.6.1.4.1.9.9.117.1.1.2.1.2.*	1:offEnvOther 2:on 3:offAdmin 4:offDenied

Enterprise ID of TRAP	Specific Type	Category	Description	Generate alert only if variable	Include in the Message ¹⁴	Variable Type
						5:offEnvPower 6:offEnvTemp 7:offEnvFan 8:failed 9:onButFanFail 10:offCooling 11:offConnector Rating 12:onButInlinePowerFail
1.3.6.1.4.1.9.9.117.2 ¹⁵	1		Module Status	1.3.6.1.4.1.9.9.117.1.2.1.1.2.* ≠ 2	Module status = 1.3.6.1.4.1.9.9.117.1.2.1.1.2.*	1:unknown 2:ok 3:disabled 4:okButDiagFailed 5:boot 6:selfTest 7:failed 8:missing 9:mismatchWithParent 10:mismatchConfig 11:diagFailed 12:dormant 13:outOfServiceAdmin 14:outOfServiceEnvTemp 15:poweredDown 16:poweredUp 17:powerDenied 18:powerCycled 19:okButPowerOverWarning 20:okButPowerOverCritical 21:syncInProgress

All other TRAPs should be filtered out.

12.3. Testing

The system should be tested during initial deployment and then annually to make sure that all components in the TRAP path are operational. SANOS allows the following test TRAPs to be triggered from the CLI:

¹⁵ Supervisor failover also results in this TRAP with status code = 1

```
Switch# test pfm test-SNMP-trap powersupply  
Switch# test pfm test-SNMP-trap temp-sensor
```

The above commands are completely non-disruptive.

13. Integration with eTrust Audit

eTrust Audit from CA is Citi standard for capturing, processing and reporting on audit events. For more details and to get answers to your questions on eTrust Audit, please visit http://pseweb.ssmb.com/?page_id=10056.

GDSE has successfully leveraged eTrust Audit framework for several storage products, and created the following documentation that will help in installing and configuring the eTrust Audit agent:

<http://engineering.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/05023-sg.pdf>

Audit logs from the MDS switch should be transported to a Solaris server via SYSLOG and capture in a text file on the server. Please see the section “Audit Trail Management” in this document for details. Once the events have been captured in the text file, the eTrust Audit UNIX Agent should be used to parse the messages in the text file and transport these to the eTrust repository. The eTrust Audit UNIX Agent configuration file, called MP file, required to correctly parse MDS audit messages is provided in appendix E.

14. Port Security

Port Security (same as McData “Port Binding”) must be enabled on all production VSANs (that means all VSANs except VSAN 1). When a host is first connected to the fabric, it will be connected to an unused port which will be a member of VSAN 1. Because there is no port security on VSAN 1, the host will be able to log on to the fabric and physical connectivity can thus be validated. The port should then be moved to a production VSAN, where Port Security is enabled, as a part of the zoning process. The host PWWN must be added to the Port Security database of the production VSAN so that the host can continue to connect to the fabric.

When switches are added to the fabric, the Port Security database of each switch at each end of the ISL must be configured with the SWWN of the partner switch. The ISL links will not come up until this is done.

Port Security eliminates the risk of a host spoofing PWWN to gain unauthorized access to LUNs of another host. It also eliminates the risk of knowingly or unknowingly adding a switch to the fabric.

15. Backup And Recovery

15.1. Switch Backup and Recovery

A script can be created on the Management Server, or any other server with SSH access to the switches to fetch the running configuration from multiple switches and dump it into individual text files. This script can be scheduled to run once every night through a scheduler. The directory where the text files are created should be configured to be backed up to tape.

The following is an example of how configuration can be fetched from the switch switch.Citi.com. “scriptuser” is the user created on the switch that uses private/public key based authentication instead of interactive authentication.

```
ssh2 scriptuser@switch.citi.com "show run" > cfg-switchname.txt
```

It is a best practice to save the active (running) configuration to the NVRAM (start-up configuration) on the switch every time the configuration is backed up. The following command should be additionally included in the script file:

```
ssh2 scriptuser@switch.citi.com "copy run start"
```

This will ensure that correct configuration is loaded if the switch gets rebooted.

Note: The MDS returns codes to indicate whether the command was successful or not, and if not for what reason. These codes can be accessed with the %errorlevel% variable:

```
ssh2 scriptuser@switch.citi.com "copy run start"  
echo Return Code = %errorlevel%
```

A return code of 0 indicates successful execution.

The details of creating a user that uses private/public key based authentication for scripting purposes is outlined elsewhere in this document.

15.2. Management Server Backup and Recovery

Management Server stores:

- Topology Map (The map displays a graphical view of the fabric)
 - o Enclosure names – The map ordinarily displays each HBA as a separate node. A server entity can be defined with multiple HBAs and labeled with the server name. This definition and label are stored on the Management Server
 - o Layout – Operator can move elements on the map around to suit his tastes. The layout is stored on the Management Server.
- Performance data

- o The Performance Manager software component constantly gathers performance data from the switches. This data can be used to identify bottlenecks and trends that can help troubleshoot issues and plan for future growth. It is also an important tool to monitor front end oversubscription with 48 port line cards. The gathered data is stored on the Management Server.

This data is stored within “C:\Program Files\Cisco Systems\MDS 9000 folder” on the Management Server. This folder should be backed up to tape on a nightly basis.

All switch configuration, zonesets, zones and device alias data is stored on every switch in the fabric, not on the Management Server. Because the CLI is a superset of the GUI, business as usual operations such as zoning can be carried out via CLI from another workstation even as the Management Server is being rebuilt.

16. Firmware Upgrades

Operations should plan to deploy new releases of SANOS for the MDS as soon as these are certified by GDSE. **Upgrade the Fabric Manager software on the Management Server before upgrading SANOS.** The vendor will provide a copy of the correct firmware either on a CD or USB flash disk, which should be copied into a directory on the Management Server¹⁶. The Firmware Upgrade wizard, available within Fabric Manager, can then be used to upgrade firmware. The wizard first transfers the image to the switch bootflash filesystem, and then initiates the upgrade.

Although the firmware update process is non-disruptive, it should still be carried out in a green zone. All switches in a fabric should be upgraded together. There should be a gap of at least a week between Fabric A and Fabric B upgrade. If issues are observed when the first fabric is upgraded, it should be downgraded to the previous version and GDSE and vendor should be notified.

17. Known Issues

- FM has a bug where certain tabs are disabled until the user clicks on one of the enabled tabs. This is scheduled to be fixed in FM 3.1.3.
- Bug ID CSCsi13231: Roles created via FM GUI can get more privileges than intended because of improper ordering of rules. Operations should check the role definitions from CLI and match these to the definitions provided above. It is scheduled to be fixed in FM 3.1.3.

¹⁶ It is a good idea for key Operations personnel to obtain a Cisco “CCO” account that will allow them to download SANOS images directly from Cisco’s website. Only GDSE certified SANOS versions should be deployed.



- Use of unlicensed features can automatically turn on demo licensing which expires after a certain time interval causing an outage. Licenses must be deployed before putting the switch into production.
- Roles can be created and deleted via FM, but cannot be edited. To edit roles, you need to use DM or CLI.
- Bug ID CSCsk55355: SANOS locks zoning database based on IP address of the workstation from where SNMP commands are being issued. In Citi's setup, multiple users can potentially simultaneously use FM on Management Server and manipulate the zoning database. The fix is scheduled for SANOS 3.2.2.
- Bug IDs CSCsj47925/CSCsj47780: Saving running to startup configuration fails while activating a zoneset via FM. The workaround is to uncheck the save running to startup checkbox when activating the zoneset. The user can save the configuration after the zoneset is activated. The zoneset is successfully activated, what fails is the configuration save. Running configuration should also be saved to startup configuration every night by using a script and scheduler as documented elsewhere in this document.

18. Appendix A: Parts List for Sample Fabric Designs

Single Tier 9506				
Description	Quantity	Cisco Part #	EMC Part # ¹⁷	HDS Part #
MDS 9506 Bundle *	2	DS-C9506-2K9	MDS-9506-V2	DS-C9506-2K9=
24 port module	8	DS-X9124	MDS-PBF-24SW	DS-X9124=
Enterprise License	2	M9500ENT1K9	MDS-ENT-9500	M9500ENT1K9=.P
FMS License	2	M9500FMS1K9	MDS-FMS-9500	M9500FMS1K9=.P
4 Gbps SW SFP (LC)	192	DS-SFP-FC4G-SW	Included on LC	DS-SFP-FC4G-SW=
4 Gbps LW SFP (LC)	0	DS-SFP-FC4G-LW	Included on LC	DS-SFP-FC4G-LW=
250VAC 20A NEMA 6-20 ¹	0	CAB-1900W-US1	MDS-PW19-US	CAB-1900W-US1=
250VAC 20A NEMA L6-20 Twist Lock ¹	2 **	CAB-1900W-US2	MDS-PW19-TWST	CAB-1900W-US2=

1. Be sure to select the appropriate power cord for your location (US, Japan, Europe, China, Australia, Israel...)

* 9506 Chassis Bundle includes: Chassis w/Fans, (2) Supervisor-2 modules, and (2) 1900W AC Power Supplies

** Power Cords come in quantities of 2

Single Tier 9509				
Description	Quantity	Cisco Part #	EMC Part #	HDS Part #
MDS 9509 Bundle *	2	DS-C9509-2K9	MDS-9509-V2	DS-C9509-2K9=
24 port module	14	DS-X9124	MDS-PBF-24SW	DS-X9124=
Enterprise License	2	M9500ENT1K9	MDS-ENT-9500	M9500ENT1K9=.P
FMS License	2	M9500FMS1K9	MDS-FMS-9500	M9500FMS1K9=.P
4 Gbps SW SFP (LC)	336	DS-SFP-FC4G-SW	Included on LC	DS-SFP-FC4G-SW=
4 Gbps LW SFP (LC)	0	DS-SFP-FC4G-LW	Included on LC	DS-SFP-FC4G-LW=
250VAC 16A NEMA 6-20 ¹	0	CAB-9K16A-US1		CAB-9K16A-US1=.P
250VAC 16A NEMA L6-20 Twist Lock ¹	2 **	CAB-9K16A-US2		CAB-9K16A-US2=.P

1. Be sure to select the appropriate power cord for your location (US, Japan, Europe, China, Australia, Israel...)

* 9509 Chassis Bundle includes: Chassis w/Fans, (2) Supervisor-2 modules, and (2) 3000W AC Power Supplies

** Power Cords come in quantities of 2

Single Tier 9513				
Description	Quantity	Cisco Part #	EMC Part #	HDS Part #
MDS 9513 Bundle *	2	DS-C9513-2K9	MDS-9513	DS-C9513-2K9=
24 port module	22	DS-X9124	MDS-PBF-24SW	DS-X9124=
Enterprise License	2	M9500ENT1K9	MDS-ENT-9500	M9500ENT1K9=.P
FMS License	2	M9500FMS1K9	MDS-FMS-9500	M9500FMS1K9=.P
4 Gbps SW SFP (LC)	528	DS-SFP-FC4G-SW	Included on LC	DS-SFP-FC4G-SW=
4 Gbps LW SFP (LC)	0	DS-SFP-FC4G-LW	Included on LC	DS-SFP-FC4G-LW=
250VAC 16A NEMA 6-20 ¹	0	CAB-9K16A-US1	MDS-PW9513-US	CAB-9K16A-US1=.P
250VAC 16A NEMA L6-20 Twist Lock ¹	2 **	CAB-9K16A-US2	MDS-PW9513-TWS	CAB-9K16A-US2=.P

1. Be sure to select the appropriate power cord for your location (US, Japan, Europe, China, Australia, Israel...)

* 9513 Chassis Bundle includes: Chassis w/Fans, (2) Supervisor-2 modules, (2) Fabric Modules, and (2) 6000W AC Power Supplies

** Power Cords come in quantities of 4

¹⁷ EMC part numbers for line cards include Short Wave optics. Part numbers are different for line cards with Long Wave optics.

Two Tier with Single Core and 2Gbps Storage Ports				
Description	Quantity	Cisco Part #	EMC Part #	HDS Part #
MDS 9513 Bundle *	12	DS-C9513-2K9	MDS-9513	DS-C9513-2K9=
24 port module	102	DS-X9124	MDS-PBF-24SW	DS-X9124=
12 port module	30	DS-X9112	MDS-PBF-12SW	DS-X9112
Enterprise License	12	M9500ENT1K9	MDS-ENT-9500	M9500ENT1K9=.P
FMS License	12	M9500FMS1K9	MDS-FMS-9500	M9500FMS1K9=.P
4 Gbps SW SFP (LC)	2808	DS-SFP-FC4G-SW	Included on LC	DS-SFP-FC4G-SW=
4 Gbps LW SFP (LC)	0	DS-SFP-FC4G-LW	Included on LC	DS-SFP-FC4G-LW=
250VAC 16A NEMA 6-20 ¹	0	CAB-9K16A-US1	MDS-PW9513-US	CAB-9K16A-US1=.P
250VAC 16A NEMA L6-20 Twist Lock ¹	12 **	CAB-9K16A-US2	MDS-PW9513-TWS	CAB-9K16A-US2=.P

1. Be sure to select the appropriate power cord for your location (US, Japan, Europe, China, Australia, Israel...)

* 9513 Chassis Bundle includes: Chassis w/Fans, (2) Supervisor-2 modules, (2) Fabric Modules, and (2) 6000W AC Power Supplies

** Power Cords come in quantities of 4

Two Tier with Dual Cores and 2Gbps Storage Ports				
Description	Quantity	Cisco Part #	EMC Part #	HDS Part #
MDS 9513 Bundle *	24	DS-C9513-2K9	MDS-9513	DS-C9513-2K9=
24 port module	204	DS-X9124	MDS-PBF-24SW	DS-X9124=
12 port module	60	DS-X9112	MDS-PBF-12SW	DS-X9112
Enterprise License	24	M9500ENT1K9	MDS-ENT-9500	M9500ENT1K9=.P
FMS License	24	M9500FMS1K9	MDS-FMS-9500	M9500FMS1K9=.P
4 Gbps SW SFP (LC)	5616	DS-SFP-FC4G-SW	Included on LC	DS-SFP-FC4G-SW=
4 Gbps LW SFP (LC)	0	DS-SFP-FC4G-LW	Included on LC	DS-SFP-FC4G-LW=
250VAC 16A NEMA 6-20 ¹	0	CAB-9K16A-US1	MDS-PW9513-US	CAB-9K16A-US1=.P
250VAC 16A NEMA L6-20 Twist Lock ¹	24 **	CAB-9K16A-US2	MDS-PW9513-TWS	CAB-9K16A-US2=.P

1. Be sure to select the appropriate power cord for your location (US, Japan, Europe, China, Australia, Israel...)

* 9513 Chassis Bundle includes: Chassis w/Fans, (2) Supervisor-2 modules, (2) Fabric Modules, and (2) 6000W AC Power Supplies

** Power Cords come in quantities of 4

Two Tiers with Dual Cores and 4Gbps Storage Ports				
Description	Quantity	Cisco Part #	EMC Part #	HDS Part #
MDS 9513 Bundle *	24	DS-C9513-2K9	MDS-9513	DS-C9513-2K9=
24 port module	180	DS-X9124	MDS-PBF-24SW	DS-X9124=
12 port module	84	DS-X9112	MDS-PBF-12SW	DS-X9112
Enterprise License	24	M9500ENT1K9	MDS-ENT-9500	M9500ENT1K9=.P
FMS License	24	M9500FMS1K9	MDS-FMS-9500	M9500FMS1K9=.P
4 Gbps SW SFP (LC)	5616	DS-SFP-FC4G-SW	Included on LC	DS-SFP-FC4G-SW=
4 Gbps LW SFP (LC)	0	DS-SFP-FC4G-LW	Included on LC	DS-SFP-FC4G-LW=
250VAC 16A NEMA 6-20 ¹	0	CAB-9K16A-US1	MDS-PW9513-US	CAB-9K16A-US1=.P
250VAC 16A NEMA L6-20 Twist Lock ¹	24 **	CAB-9K16A-US2	MDS-PW9513-TWS	CAB-9K16A-US2=.P

1. Be sure to select the appropriate power cord for your location (US, Japan, Europe, China, Australia, Israel...)

* 9513 Chassis Bundle includes: Chassis w/Fans, (2) Supervisor-2 modules, (2) Fabric Modules, and (2) 6000W AC Power Supplies

** Power Cords come in quantities of 4

19. Appendix B: Glossary

Term	Description	McData Equivalent (if any)
BAU	Business As Usual; day to day procedures such as provisioning of storage	
BISO	Business Information Security Officer. Each business unit has its own BISO. The BISO is ultimately responsible for interpreting CISS and approving security measures.	
CEP	Common Extranet Platform – a secure IP network isolated from the corporate network by a firewall. Citi uses CEP to host applications that need partner connectivity.	
CISS	Citi Information Security Standards	
CLI	Command Line Access	
COB	Continuity of Business	
DM	Device Manager: GUI Software used to manage switch specific features	Element manager within Connectrix Manager
EMC	EMC Corporation http://emc.com	
EP	Exposure Profile: As a part of security assessment process, a risk profile must be built for all products.	
FC	Fibre Channel	
FM	Fabric Manager: GUI Client used to manage MDS fabrics	Connectrix Manager client
FMS	FM Server: Manages access from multiple simultaneous clients. FM clients connect to this server.	Connectrix Manager server
FSPF	Fabric Shortest Path First protocol: It calculates the best path between switches, establishes routes across the fabric and calculates alternate routes in event of a failure or topology change.	FSPF
FTE	Full Time Employee	
GDN	Global Data Network. This is Citi's corporate network or Intranet	
GDSE	Global Distributed Storage Engineering	
Gen2	Generation 2 hardware	
GUI	Graphical User Interface	
ICQ	Information Security Compliance Questionnaire: As a part of the security assessment process, ICQ must be completed for every product. The ICQ helps identify gaps with CISS.	
ISL	Inter switch link	ISL
IVR	Inter-VSAN Routing	
HDS	Hitachi Data Systems http://hds.com	
MPSM	Multi Protocol Services Module	

Term	Description	McData Equivalent (if any)
Ops, Operations	Operations: Regional teams responsible for operating Citi SANs in various datacenters	
PCM	Process Control Manual: this is where Operations document their processes. Each region has its own PCM.	
Port Channel	A collection of ISLs where individual ISL failure does not trigger FSPF convergence	No such feature
Port Security	Tie switch port to node PWWN or switch WWN to safeguard from unauthorized access	Port Binding
RA	Risk Acceptance: RA must be approved by management if product with security gaps is being deployed in production.	
SA	System Administrator: Person who manages servers	
SAN	Storage Area Network	
SANOS	Switch firmware	E/OS
SOE	Citi Standard Operating Environment	
SSM	Storage Service Module	
Sup2	Generation 2 supervisor module	CTP
Traffic Engineering	Manually allocating VSANs to ISLs/Port Channels for optimal utilization, applying QoS to prioritize traffic through the network, and manually changing FSPF cost to send traffic down a different path to meet SLA.	
Trunk, or Trunked ISL VSAN	An ISL that is configured to carry multiple VSANs Virtual SAN	Do not confuse this with "Open Trunking", which is McData software to load balance ISLs

20. Appendix C: Resolving Application Conflicts

The Cisco MDS management applications can co-exist with other storage management applications such as EMC Connectrix Manager, SanScreen RAU etc. Consolidating applications on to a single server can reduce costs. In order to make this work, application conflicts have to be identified and resolved. Two areas where applications can conflict are:

1. Java runtime version
2. TCP and UDP ports that the applications listen on

	Application vendor	Can application be configured to use its own JRE (server will have more than one version installed)? If this is a "NO", this app cannot interop with any other app that also has a "NO"	Fixed TCP ports that cannot be reconfigured	Fixed UDP ports that cannot be reconfigured
CM 8.7.1 Client	EMC	N/A - App uses its own JRE	None	None
CM 8.7.1 Server (CM on SOE Server)	EMC	N/A - App uses its own JRE	80, 1635, 1638, 1639, 1645, 51510, 51511, 51512, 51513	162, 1024, 1041, 1066, 1067, 1069, 4033
Cisco FM client, FMS, Perf. Manager 3.1.2	Cisco	YES		514
Cisco ACS 4.1.3 Server for MDS	Cisco	N/A - App does not use JRE	49, 2000, 2001, 2002	1141, 1645, 1646, 1812, 1813
HDS Hi-Track 3.9 for MDS	HDS	YES	None	None
Navisphere Server and Client	EMC	NO	2162, 2163, 4670	None
ESRS	EMC	N/A - App does not use JRE	3011, 3030	None
ESRS Policy Manager & Tomcat	EMC	N/A - App uses its own JRE	8005, 8090	None
SanScreen Remote Acquisition Unit 3.5	Onaro	N/A - App uses its own JRE	1352, 5679, 12123	162
SanScreen Local Acquisition Unit 3.5	Onaro	N/A - App uses its own JRE	9009, 9010, 12123	None
SanScreen Explorer (Client) 3.5	Onaro	N/A - App uses its own JRE	None	None
SanScreen Server 3.5	Onaro	N/A - App uses its own JRE	1098, 1099, 1143, 1146, 1351, 1883, 2143, 2229, 2919, 3306, 3789, 4444, 4445, 8083, 8086, 8090, 8092, 8093, 33333, 50000	None

	Application vendor	Can application be configured to use its own JRE (server will have more than one version installed)? If this is a "NO", this app cannot interop with any other app that also has a "NO"	Fixed TCP ports that cannot be reconfigured	Fixed UDP ports that cannot be reconfigured
ECC 5.2 SP4 Host and CX Agent	EMC	N/A - App does not use JRE	1104, 6369, 10444	None
ECC 5.2 SP4 Host and HDS Agent	EMC	N/A - App does not use JRE	11023, 10444	None
eTrust Audit 8.2sp2 Agent	CA	N/A - App does not use JRE	5250, 8025	8024, 8025
HDS HDvM Server and Client v3.0 and above	HDS	NO	21, 80, 1099, 2000, 2001, 2443, 3050, 3060, 45001-49000, 51099, 51100	161, 162
HDS Storage Navigator Client v3.0 and above	HDS	NO	None	None
3rd Party SYSLOG Server for Windows (Not GDSE certified)		N/A - App does not use JRE	None	514
FileCensus 3.4.2/4.1	Intermine	Yes	None	None
Operations Manager 3.5	NetApp	N/A - App does not use JRE	22, 23, 25, 80, 443, 514, 4092, 4093, 8443, 8448, 10000	161, 162
McData IPS SAN Routers/Sanvergence	EMC	TBD	20, 21, 80	69, 123, 161, 162, 37009, 37010
Solutions Enabler with SYMAPI Server	EMC	N/A - App does not use JRE	2707	None

MDS management applications can be configured to use a specific Java version and custom TCP/UDP ports.

20.1. Configure Path to Java Runtime

1. Install JRE version 1.5 or higher. At the time of writing of this document, Java Development Kit v1.5.0_06 is available from GDSGOLD distribution server as SPAC ID "jks15060". Please consult with your SA for the latest certified version of Java.
2. Edit¹⁸ all batch files (*.BAT) in the directory "C:\Program Files\Cisco Systems\MDS 9000\bin\"¹⁹ file and set the "JAVA" and "JAVACMD" variables to point to the "javaw.exe" and "java.exe" files respectively:

¹⁸ Make sure to create a backup of any file that you edit so that configuration can be restored if mistakes are made

¹⁹ "C:\Program Files\Cisco Systems\MDS 9000" is the default install location for MDS applications. The location would be different if the applications are installed from SPAC.

```
set JAVA= C:\apps_srv\jre1.5.0_06\publicjre\bin\javaw.exe
set JAVACMD= C:\apps_srv\jre1.5.0_06\publicjre\bin\java.exe
```

3. Edit the all *.conf files within the “C:\MDS9000\conf” directory and “C:\MDS9000\conf\FMWebClient.conf” and correct the “wrapper.java.command” variable to the new path to “javaw.exe”:

```
wrapper.java.command=C:\apps_srv\jre1.5.0_06\publicjre\bin\javaw.exe
```

After making these changes, use Windows Services control applet to restart the following services:

- ✓ Cisco MDS Database Server
- ✓ Cisco MDS Fabric Manager
- ✓ Cisco MDS Fabric Manager Web Server

20.2. Configure TCP/UDP Ports

Listening Program	Default Port	How to Change the Port
FMS – listens for client connections	TCP/9099	Edit “C:\Program Files\Cisco Systems\MDS 9000\server.properties”. Change “server.port”. Restart “Cisco MDS Fabric Manager” service after saving changes.
FMS – sends and receives data	TCP/9100	Edit “C:\Program Files\Cisco Systems\MDS 9000\server.properties”. Change “server.data.port”. Restart “Cisco MDS Fabric Manager” service after saving changes.
FMS – listen for SNMP TRAPS	UDP/2162	Edit “C:\Program Files\Cisco Systems\MDS 9000\server.properties”. Change “trap.port”. Restart “Cisco MDS Fabric Manager” service after saving changes.
FMS – listen for SYSLOG messages	UDP/514	Cannot be changed!
Performance Manager Web Server	TCP/80	Select port during install. Once installed, it can be changed by editing “C:\Program Files\Cisco Systems\MDS 9000\tomcat\conf\server.xml”. In the “Connector” configuration, set the “port” parameter to the desired value. Do this for both HTTP and HTTPS connector definitions. Restart the “Cisco MDS Fabric Manager Web Server” service after saving the changes.

21. Appendix D: Switch Configuration (“Template”)

! Script to configure Cisco MDS switch running SANOS 3.1.2

! by Parul Jain parul.k.jain@citi.com

! If the switch has been configured before use the write erase and reload commands to

! clear the configuration before running this script

! Change items in **red** to match the switch and environment

! Copy the script to the switch and then execute using the script-run command

! Use Console port to run the script because it changes IP address and IP ACL

! Enter configuration mode

config

! Configure banner limit is 80 chars

banner motd # Unauthorized use of this system is prohibited #

! Logging related configuration

! Enable logging configuration distribution via CFS

logging distribute

! SYSLOG server IP address and facility

logging server **10.40.42.200** 6 facility local1

logging level authpriv 5

logging level aaa 6

logging commit

! Set up time zone and automatic DST if applicable

clock timezone **EST -5 0**

clock **summer-time EDT 2 Sunday Mar 02:00 1 Sunday Nov 02:00 60**

! Configure roles

! Enable role distribution via CFS

role distribute

! Roles

role name storage_admin

rule 1 permit config

rule 2 permit debug

rule 3 permit show

rule 4 permit exec

rule 5 deny config feature aaa

rule 6 deny config feature radius-server

rule 7 deny config feature tacacs+

rule 8 deny config feature tacacs-server

rule 9 deny config feature telnet

rule 10 deny config feature ssh

```
rule 11 deny debug feature aaa
rule 12 deny debug feature tacacs+
rule 13 deny config feature logging
exit
```

```
role name vendor
rule 1 permit show
rule 2 permit exec feature attach
rule 3 permit exec feature clear
rule 4 permit exec feature debug
rule 5 permit exec feature undebug
rule 6 permit exec feature dir
rule 7 permit exec feature fcping
rule 8 permit exec feature fctrace
rule 9 permit exec feature terminal
rule 10 permit exec feature delete
rule 11 permit exec feature copy
rule 12 permit exec feature install
rule 13 permit exec feature ping
exit
```

```
role name script
rule 1 permit show
rule 2 permit exec feature attach
rule 3 permit exec feature clear
rule 4 permit exec feature debug
rule 5 permit exec feature undebug
rule 6 permit exec feature dir
rule 7 permit exec feature fcping
rule 8 permit exec feature fctrace
rule 9 permit exec feature terminal
exit
```

```
role name facility
rule 1 permit show feature fcns
rule 2 permit show feature flogi
vsan policy deny
permit vsan 1-1
exit
role commit
```

```
! Enable SSH access
ssh key rsa 1024 force
ssh server enable
```

```
! Synchronize time with NTP for accurate log entry time
```

```
ntp distribute
```

```
ntp server 192.193.215.65
```

```
ntp server 192.193.215.69
```

```
ntp commit
```

```
! IP Access Control List: Protect switch from unauthorized access
```

```
! Allow full access from Primary Management Server(s)
```

```
ip access-list inbound1 permit ip 10.40.42.19 0.0.0.0 any
```

```
ip access-list inbound1 permit ip 10.40.42.200 0.0.0.0 any
```

```
! Allow SSH access (tcp) from other servers. Add as many as necessary.
```

```
!*** CLI only via SSH Servers ***
```

```
ip access-list inbound1 permit tcp 169.185.200.90 0.0.0.0 any eq port ssh
```

```
ip access-list inbound1 permit tcp 169.185.200.91 0.0.0.0 any eq port ssh
```

```
! Allow Hi-Track server (HDS only) access via SNMP
```

```
ip access-list inbound1 permit udp 10.40.42.200 0.0.0.0 any eq port snmp
```

```
!*** NTP servers, use 2 for backup ***
```

```
ip access-list inbound1 permit udp 192.193.215.65 0.0.0.0 any eq port ntp
```

```
ip access-list inbound1 permit udp 192.193.215.69 0.0.0.0 any eq port ntp
```

```
!*** Allow SSH from CitiVPN pools for Vendor Remote Access ***
```

```
ip access-list inbound1 permit tcp 172.23.33.64 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.37.64 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.45.64 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.49.64 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.65.64 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.97.64 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.109.64 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.244.128 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.228.128 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.215.128 0.0.0.63 any eq port ssh
```

```
ip access-list inbound1 permit tcp 172.23.199.128 0.0.0.63 any eq port ssh
```

```
! Allow the world to ping me
```

```
ip access-list inbound1 permit icmp any any
```

```
! Allow SanScreen server access via SNMP
```

```
ip access-list inbound1 permit udp 10.40.42.37 0.0.0.0 any eq port snmp
```

```
! SNMP related configuration
```

```
snmp-server contact GDSE
```

```
snmp-server location Lab 10, Warren, NJ, USA
```

```
! Allow SanScreen read-only SNMP v1 access
```

```
snmp-server community sansscreen group network-operator
```

! TRAP collector server IP address, community (default public) and

! UDP port (default 162) will be provided by ESS

```
snmp-server host 10.40.42.200 public udp-port 162
```

```
snmp-server host 168.109.182.108 public udp-port 162
```

! Enable these TRAP categories for monitoring

```
snmp-server enable traps license
```

```
snmp-server enable traps entity
```

```
snmp-server enable traps fcdomain
```

```
snmp-server enable traps zone
```

! Enable the following alerts on **core switches ONLY**,

! You do not want to be alerted every time a host is reboot or shutdown for maint.

! If your not using core-edge topology, do not enable this; instead

! enable on a per interface basis (sample not provided in template)

```
snmp-server enable traps link cisco
```

! HDS supported switch section

! Allow SNMP v1 read-only access from Hi-Track

```
snmp-server community hitrack group network-operator
```

! End HDS supported switch section

! Configure management interface

```
interface mgmt0
```

```
switchport speed 100
```

```
ip address 10.40.42.109 255.255.255.0
```

! Warning: the following will apply ACL to interface

! Incorrect ACL will lock you out instantly - recover from console port

```
ip access-group inbound1 in
```

```
exit
```

! Configure default gateway

```
ip default-gateway 10.40.42.2
```

! Configure switch name

```
switchname 2r11-mds9500-02
```

! Disable telnet for security reasons

```
no telnet server enable
```

! There is no need to enable Cisco Discovery Protocol CDP

```
no cdp enable
```

! This will configure VSANs for a default and one production VSAN per fabric

! VSAN id 2 = “Fabric A”

! VSAN id 3 = “Fabric B”

! Please customize if you require more production VSANs

vsan database

vsan 2 name "FABRIC_A"

exit

! Enable “enhanced” zoning mode for all production VSANs

zone mode enhanced vsan 2

! Domain IDs related configuration

! Enable CFS distribution for domain IDs to eliminate possibility

! of duplicates and resulting isolation

fcdomain distribute

! Please see Domain ID design guide

fcdomain domain 2 static vsan 2

fcdomain commit vsan 2

! restart fcdomain services for changes to take effect

fcdomain restart disruptive vsan 2

! FCIDs should be made persistent

fcdomain fcid persistent vsan 2

! Reserve a block of domain IDs for VSANs

fcdomain allowed 1-12 vsan 2

fcdomain commit vsan 2

! Configure interfaces

! Enable all ports by default so that facility can test new connections

no system default switchport shutdown

! We do not want to automatically send all VSANs down every ISL

system default switchport trunk mode off

! We need to configure all ports as F ports so that no damage is done if

! switches are accidentally interconnected

interface fc2/1-24, fc3/1-48, fc4/1-12, fc5/1-12

switchport mode F

exit

! Device alias related configuration

! Disable device alias enhanced mode because changing device alias will cause

! automatic change to active zoneset in enhanced mode

device-alias distribute

```
no device-alias mode enhanced
device-alias commit
```

```
! Zoning related configuration
! Drop traffic when not zoned for security
no system default zone default-zone permit
```

```
! Distribute all (active or not) zonesets to all switches for COB
system default zone distribute full
```

```
! Port security related configuration
! Enable port security feature
port-security enable
```

```
! Do not distribute port security via CFS
no port-security distribute
```

```
! Port channel (ISL) configuration, use ports from 12 port line cards only.
! Repeat the following configuration for as many port channels as you need
```

```
interface fc5/5, fc4/5, fc5/6, fc4/6
  switchport description "To switch 2r11-mds9500-01"
  switchport mode E
  channel-group 4
  no shut
  exit
interface port-channel 4
  switchport trunk mode on
  channel mode active
  switchport trunk allowed vsan 1
  switchport trunk allowed vsan add 2
  no shut
  exit
```

```
! Configure port security for port channel configured above
! Obtain swwn of peer switch with "sh wwn switch" command
port-security database vsan 2
  swwn 20:00:00:0d:ec:25:0c:80 interface port-channel 4
  exit
port-security activate vsan 2 no-auto-learn
```

```
! Authenticate to IAS via RADIUS
! This should only be configured after all instruction in section 7.1 of Solutions Guide
! have been executed
! RADIUS server host is Management Server where IAS is running
! Use the Key that was configured in IAS
```

```
radius-server host 10.40.42.200 key cisco123
aaa group server radius radius-group1
  server 10.40.42.200
exit
aaa authentication login default group radius-group1

! Console access should not be authenticated via ACS
! Console can be used for recovery from bad ACS
aaa authentication login console local

! Use MSCHAP v2 protocol for authentication with IAS
aaa authentication login mschap enable

! End Authenticate to IAS via RADIUS section

! Enable DNS lookup for convenient SFTP transfers
ip domain-name lookup
ip name-server 10.42.32.11 146.128.201.218
ip domain-name nam.nsroot.net

! Enable NPIV to support HP C Class Blade Center
npiv enable

! Exit config mode
exit

! Let the switch digest the configuration changes
sleep 30

! Save the configuration
copy run start

! End of template
```

22. Appendix E: eTrust Audit MP File

```

*****
;
***
;Project : eTrust Audit 1.5 SP3
;Module  : Cisco MDS Log via Syslog
;File    : CiscoMDS.mp
;Purpose : Message parsing file for UNIX syslog containing Cisco MDS messages
*****
;
***
;Developed By : Kery Hines for Unix eTrust Audit 1.5 SP3
;Modified By  : Kery Hines Feb 14, 2007
*****
;
***
;
;
;-----
Tokens
{
Date
{
Type = datetime
format = [0-9]+ [a-zA-Z]+ [0-9]+ [0-9]+:[0-9]+:[0-9]+
DateTimeFormat = %Y %b %d %T
}
MDSMessage
{
format = .*
}
SwitchName
{
format = [a-zA-Z0-9_-]*
}
Vsan
{
format = [a-zA-Z0-9_-]*
}
<Misc> = <_rest>
}
;-----
TranslateTbl
{
}
;-----
Records
{
;

```

```
;Categories
;
;Pattern 1 -----
;
;Feb 8 17:20:26 [10.40.53.54.2.2] : 2007 Feb 08 17:20:26 EST:
;
MDS_Main_Rec
{
Name = MDS_Main_Rec
KeyVal = 0
Type = CATEGORY
Regex = [a-zA-Z]+ [0-9]+ [0-9]+:[0-9]+:[0-9]+ \[[0-9.]+\] : <Date> [a-zA-Z]+: <_rest>
Key = MDS_Main_Rec
ReplaceSpace = TRUE
}
;
;Pattern Catch all record -----
;
MDSCatch_All
{
Name = MDSCatch_All
KeyVal = 0
Type = CATEGORY
Regex = [a-zA-Z]+ [0-9]+ [0-9]+:[0-9]+:[0-9]+ \[[0-9.]+\] : <Date> [a-zA-Z]+: <_rest>
Key = MDSCatch_All
ReplaceSpace = TRUE
}
;
;Records
;
;Pattern 1a -----
;
; %PORT-5-IF_DOWN_LINK_FAILURE: %$VSAN 2%$ Interface fc2/3 is down (Link
failure)
;
Key_MDS_Mess_with_Vsan
{
Name = Key_MDS_Mess_with_Vsan
KeyVal = MDS_Main_Rec
Type = RECORD
Regex = <SwitchName> %<MDSEvent>: %$<Vsan>%$ <MDSMessage>
Key =
ReplaceSpace = TRUE
AddToken1 = Category:MDS VSAN Message
AddToken2 = Log:CiscoMDS
```

```

    AddToken3 = Src:Switch <SwitchName>, <Vsan>, Event - <MDSEvent>, Message -
<MDSMessage>
}
;
;Pattern 1b -----
;
; %DAEMON-3-SYSTEM_MSG: error: PAM: Authentication failure for admin from
10.40.42.16
;
Key_MDS_Mess_without_Vsan
{
    Name = Key_MDS_Mess_without_Vsan
    KeyVal = MDS_Main_Rec
    Type = RECORD
    Regex = <SwitchName> %<MDSEvent>: <MDSMessage>
    Key =
    ReplaceSpace = TRUE
    AddToken1 = Category:MDS Standard Message
    AddToken2 = Log:CiscoMDS
    AddToken3 = Src:Switch <SwitchName>, Event - <MDSEvent>, Message - <MDSMessage>
}
;
;Pattern 1c -----
;
; snmpd: SNMPD_SYSLOG_CONFIG_I: Configuration update from 1118_10.40.42.16
user/community name : admin
;
Key_MDS_Mess_Other
{
    Name = Key_MDS_Mess_Other
    KeyVal = MDS_Main_Rec
    Type = RECORD
    Regex = <SwitchName> <MDSEvent>: <MDSMessage>
    Key =
    ReplaceSpace = TRUE
    AddToken1 = Category:MDS Other Message
    AddToken2 = Log:CiscoMDS
    AddToken3 = Src:Switch <SwitchName>, Event - <MDSEvent>, Message - <MDSMessage>
}
;
;Pattern Catch all record -----
;
KeyMDSCatch_All
{
    Name = KeyMDSCatch_All
    KeyVal = MDSCatch_All

```



```
Type = RECORD
Regex = <Misc>
Key =
ReplaceSpace = TRUE
AddToken1 = Category:MDS Catch All
AddToken2 = Log:CiscoMDS
AddToken3 = Src:<Misc>
}
}
```