



Global Distributed Storage Engineering

SAN Secure Configuration Guide

GDSE-04004-S

Secure Configuration Guide

1.4

Document Classification: INTERNAL

1. Version Control

Version	Date	Author	Reviewed	Comments
0.2	30-March-04	Parul Jain	GDSE, Ed Feinstein, Janet Cugini	Various
0.5	16-April-04	Parul Jain	Global Storage Task Force	Various
0.6	07-May-04	Parul Jain	Bob Small	Various
1.0	10-May-04	Parul Jain		Release
1.1	11-Aug-04	Burt Giron	Operational Owners	Appended Symmetrix/DMX Security configuration Section 11.3
1.2	8-Sep-04	Parul Jain	-	Appended reference to secure management network for Clariion Section 14.2
1.3	3-Dec-04	Scott Torgerson	GDSE	Appended SANtegrity Configurations Sections 9.7 and 9.8
1.4	14-Dec-04	Parul Jain	-	Appended new design for vendor remote access to Symmetrix Section 15.3.1
1.4.1	21-Dec-04	Burt Giron	-	Appended Symmetrix/DMX VCMDB_restricted_access=enable host impact Section 11.3.1.4

2. Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, CITIGROUP and the Umbrella Device are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

3. Contact

Please address any comments or questions regarding the information contained in this document via email to the “*GT Global Distributed Storage Engineering” distribution list or alternatively to gdse@citigroup.com.

4. Latest Versions

It is recommended that the latest version of the document be used from the GDSE website <http://gdse.ny.ssmb.com>. Newer versions may include expanded scope, or comments on issues discovered after deployment.

Table Of Contents

1. VERSION CONTROL	2
2. LEGAL NOTICE	3
3. CONTACT	3
4. LATEST VERSIONS.....	3
5. INTRODUCTION.....	9
6. SCOPE.....	9
6.1. PRODUCTS.....	9
6.2. SECURITY STANDARDS.....	9
7. INFORMATION CLASSIFICATION CERTIFICATION.....	10
8. INTRODUCTION TO STORAGE AREA NETWORKS.....	11
8.1. COMMON SAN TOPOLOGIES.....	11
8.1.1. ENTERPRISE TIER SAN	11
8.1.2. MID TIER SAN.....	13
9. MCDATA SWITCH	16
9.1. INTRODUCTION.....	16
9.2. IDENTIFICATION AND AUTHENTICATION.....	16
9.3. AUTHORIZATION AND ACCESS CONTROL	18
9.4. CONFIDENTIALITY AND INTEGRITY	18
9.5. INCIDENT DETECTION AND RESPONSE.....	19
9.6. ADMINISTRATION.....	19
9.7. SECURE FABRIC CONFIGURATION - SANTEGRITY	20
9.7.1. SANTEGRITY PORT BINDINGS	21
9.7.2. SANTEGRITY FABRIC BINDINGS	24
9.8. SANTEGRITY OPERATIONAL CHANGES	26
9.8.1. ADDING NEW STORAGE/SERVER CONNECTIONS TO THE SWITCH.....	26
9.8.2. ADDING NEW SWITCHES TO THE FABRIC	27
9.8.3. ADDING ADDITIONAL ISLs FROM EXISTING SWITCHES	28
9.8.4. REMOVING HOSTS FROM SWITCHES	28
9.8.5. REMOVING ISLs FROM SWITCHES.....	28
9.8.6. REMOVING SWITCHES FROM A FABRIC.....	29
10. CONNECTRIX MANAGER	29
10.1. INTRODUCTION.....	29
10.2. IDENTIFICATION AND AUTHENTICATION.....	30
10.3. AUTHORIZATION AND ACCESS CONTROL	30
10.4. CONFIDENTIALITY AND INTEGRITY	30
10.5. INCIDENT DETECTION AND RESPONSE.....	30

10.6.	ADMINISTRATION	30
11.	SYMMETRIX ARRAY	34
11.1.	INTRODUCTION.....	34
11.2.	IDENTIFICATION AND AUTHENTICATION	34
11.3.	AUTHORIZATION AND ACCESS CONTROL	34
11.3.1.	VOLUME CONTROL MASKING DATABASE (VCMDB)-Host/HBA RESTRICTION.....	35
11.3.1.1.	“VCMDB_RESTRICTED_ACCESS” CONFIGURATION AND SETUP	36
11.3.1.2.	HOST IMPACT ENABLING “VCMDB_RESTRICTED_ACCESS”	42
11.3.1.3.	ADDING AND REMOVING SAN MANAGEMENT HOSTS	43
11.3.1.4.	DISABLING “VCMDB_RESTRICTED_ACCESS”	43
11.3.2.	SYMACL – SYMMETRIX/DMX HOST ACCESS CONTROL MANAGEMENT	44
11.3.2.1.	SYMACL SYMMETRIX/DMX SETUP	47
11.3.2.2.	DEFAULT CONFIGURATION	48
11.3.2.3.	ACCESS GROUP MANAGEMENT.....	49
11.3.2.3.1.	ADD USER ACCESS IDS TO A GROUP	50
11.3.2.3.2.	ACCESS GROUP MAINTENANCE	51
11.3.2.4.	DEVICE POOL MANAGEMENT.....	52
11.3.2.5.	ACE/ACLs MANAGEMENT.....	53
11.3.2.6.	ACCESS CONTROL INFORMATION.....	57
11.3.2.7.	SYMACL BACKUP AND RESTORE.....	57
11.3.2.7.1.	SYMACL BACKUP	57
11.3.2.7.2.	SYMACL RESTORE.....	59
11.3.3.	STRATEGY FOR HOSTS REQUIRING BCV/SYMMIR CONTROLS.....	59
11.3.4.	STRATEGY FOR HOSTS REQUIRING SRDF CONTROLS	60
11.3.5.	GDSE RECOMMENDED ACCESS CONTROL STRATEGY.....	60
11.4.	CONFIDENTIALITY AND INTEGRITY	61
11.5.	INCIDENT DETECTION AND RESPONSE.....	61
11.6.	ADMINISTRATION	61
12.	SOLUTIONS ENABLER	62
12.1.	INTRODUCTION.....	62
12.2.	IDENTIFICATION AND AUTHENTICATION	62
12.3.	AUTHORIZATION AND ACCESS CONTROL	63
12.4.	CONFIDENTIALITY AND INTEGRITY	64
12.5.	INCIDENT DETECTION AND RESPONSE.....	64
12.6.	ADMINISTRATION	64
13.	BROCADE SWITCH	65
13.1.	INTRODUCTION.....	65
13.2.	IDENTIFICATION AND AUTHENTICATION	65
13.3.	AUTHORIZATION AND ACCESS CONTROL	65
13.4.	CONFIDENTIALITY AND INTEGRITY	66
13.5.	INCIDENT DETECTION AND RESPONSE.....	66
13.6.	ADMINISTRATION	66

14.	CLARIION ARRAY AND NAVISPHERE	69
14.1.	INTRODUCTION.....	69
14.2.	IDENTIFICATION AND AUTHENTICATION	70
14.3.	AUTHORIZATION AND ACCESS CONTROL	70
14.4.	CONFIDENTIALITY AND INTEGRITY	71
14.5.	INCIDENT DETECTION AND RESPONSE	71
14.6.	ADMINISTRATION	72
15.	REMOTE FAULT MANAGEMENT	73
15.1.	INTRODUCTION.....	73
15.2.	IDENTIFICATION AND AUTHENTICATION	73
15.3.	AUTHORIZATION AND ACCESS CONTROL	75
15.3.1.	VENDOR REMOTE ACCESS FOR SYMMETRIX	75
15.4.	CONFIDENTIALITY AND INTEGRITY	76
15.5.	INCIDENT DETECTION AND RESPONSE	76
15.6.	CONFIDENTIALITY AND INTEGRITY	77
15.7.	INCIDENT DETECTION AND RESPONSE	77
15.8.	ADMINISTRATION	77
16.	REFERENCES.....	78
17.	APPENDICES	79
17.1.	APPENDIX A: ROLES WITHIN THE NAVISPHERE APPLICATION.....	79
17.2.	APPENDIX B: NAVISPHERE LOGS	80
17.3.	APPENDIX C: ROLES WITHIN THE CONNECTRIX MANAGER APPLICATION	81
17.4.	APPENDIX D: CONNECTRIX MANAGER LOGS.....	82
17.5.	APPENDIX E: SYMMETRIX ARRAY LOGS.....	84
17.6.	APPENDIX F: BROCADE SWITCH LOGS.....	85
17.7.	APPENDIX G: CITIGROUP INFORMATION SECURITY STANDARDS	87

List of Figures

Figure 1 Enterprise Tier SAN	12
Figure 2 Mid Tier SAN.....	14
Figure 3 Secure Topology for McData Switch.....	17
Figure 4 Disabling the Telnet and Web server on the McData switch	19
Figure 5 SNMP Agent configuration for the McData switch	20
Figure 6 Bind All WWNs.....	22
Figure 7 Bind All Ports To Attached WWNs	23
Figure 8 Manual Port Binding Entries.....	24
Figure 9 Fabric Membership List.....	25
Figure 10 Disabling the SNMP Agent on Connectrix Manager.....	31
Figure 11 Restricting Access to Connectrix Manager	33
Figure 12 - EMC Symmetrix detailed version information	36
Figure 13 - EMC Solutions Enabler detailed version information	37
Figure 14 - Solutions Enabler "symImf" utility.....	38
Figure 15 - VCMDB_restricted_access command file.....	39
Figure 16 - VCMDB HBA assignments	39
Figure 17 - "symconfigure" preview stage	40
Figure 18 - "symconfigure" prepare stage.....	40
Figure 19 - "symconfigure" commit stage.....	41
Figure 20 - "symcfg list -lock"	42
Figure 21 - "symcfg discover" - update local SYMAPI database	42
Figure 22 - "VCMDB_restricted_access" disable command file.....	44
Figure 23 - Sample Symmetrix/DMX "symacl" configuration.....	46
Figure 24 – Host and Symmetrix/DMX variables required for initial setup of symacl.....	47
Figure 25 - "SYMACL -unique" HOST ID	48
Figure 26 - symacl creating accgroup command file syntax.....	49
Figure 27 - symacl adding host Access ID command file syntax.....	50
Figure 28 - symacl adding User Access ID command file syntax.....	51
Figure 29 - symacl Delete Access Group command file syntax	52
Figure 30 - symacl create accpool command file syntax.....	52
Figure 31 - symacl add dev to accpool command file syntax	53
Figure 32 - granting symacl rights command file syntax	56
Figure 33 - symacl backup file command file syntax	58
Figure 34 - symacl database -restore command syntax.....	59
Figure 35 Secure Topology for Solutions Enabler.....	63
Figure 36 Disabling the SNMP agent on the Brocade switch	67
Figure 37 Enabling the SNMP agent on the Brocade switch.....	68
Figure 38 Configuring privileged users on Clariion.....	71
Figure 39 Securing Corporate Network from SAN Network	75
Figure 40 Tactical Solution for Vendor Remote Access to Symmetrix	76
Figure 41 Navisphere Audit Log.....	80
Figure 42 Connectrix Manager Logs	82
Figure 43 Connectrix Manager Audit Log.....	83

Figure 44 Brocade switch logs collected on a syslog server 85

Figure 45 Brocade switch logs collected on a SNMP management station 86

5. Introduction

Storage Area Networks (“SAN”) offer high performance, reliable and manageable storage for critical company data. The SAN processes confidential information from across businesses, and is a critical component of the technology infrastructure.

This guide establishes the configuration of various SAN components so as to meet the Citigroup Information Security Standards (“CISS”).

This guide, together with the Information Security (“IS”) Product TRAM and the SAN Technical TRAM, provides the foundation for the assessment of operational risk associated with production SAN environments.

6. Scope

6.1. Products

The following SAN components are in scope:

- Connectrix Manager 6.3.1
- McData Switch E/OS 4.01.04
- SymmRemote 2.04
- Brocade 3800 Firmware 3.02m
- EMC Clariion FC and CX series
- Navisphere 6.4.0
- EMC Symmetrix 3x30, 8000 series, DMX 1000 and DMX 2000
- Solutions Enabler 5.2

6.2. Security Standards

Citigroup Information Security Standards (“CISS”) have been used as standards. A summary has been enclosed in appendix G. For latest versions and more details, please refer to the Information Security Services (“ISS”) website at <http://www.citigroup.net/informationsecurityservices/>.

7. Information Classification Certification

The SAN is infrastructure, and thus will be managed towards a class 'C' certification¹. Therefore, the SAN can process and store information classified as "public", "internal" and "confidential" only. Information classified as "restricted" or "highly confidential" cannot be processed on the SAN unless adequate controls, such as encryption, are built into the application.

¹ Please refer to <http://www.citigroup.net/tie/seceng/documents/InfrastructureClassificationRatingsFINALv2.doc>, page 5.

8. Introduction to Storage Area Networks

A SAN is a high-speed special-purpose network that interconnects different kinds of data storage devices with servers (“host”). The SAN uses Fibre Channel (“FC”) technology for interconnecting devices. The most common use of the SAN within the company is to provide high performance and highly available disk storage to hosts that run business applications. The SAN also provides services that enable continuity of business. Such services include data replication, data migration and backup.

A host needing access to the SAN is equipped with one or more host bus adaptors (“HBA”), and is then connected to fiber-optic cabling. The cabling terminates on one or more FC switches that are responsible for routing data between devices within the FC network. If the host needs access to a resource such as a disk drive, it is assigned a logical disk (“LUN”) from a storage array connected to the SAN.

The SAN is a shared facility that is used by multiple business units. In order to maintain confidentiality, it is important to authenticate and authorize access to data. Because SAN resources are assigned to hosts rather than individual users, the authorization is based on the identity of the host, rather than the identity of the user that runs the applications on the host.

8.1. Common SAN Topologies

SAN topologies vary from site to site. In the New York area, two distinct topologies are in use, the “Enterprise Tier SAN” and the “Mid Tier SAN”. The following details these topologies in an effort to highlight control issues within SANs.

8.1.1. Enterprise Tier SAN

The Enterprise Tier SAN is designed to deliver highest performance for enterprise applications. It comprises of the following components:

<i>EMC Symmetrix storage arrays</i>	Provide highly available and high performance disk storage to hosts
<i>McData fibre channel switches</i>	Provide highly available and scalable connectivity between the hosts and the array ports
<i>Host Bus Adaptors</i>	Enable hosts to connect to the Fibre Channel network
<i>Interconnecting hardware</i>	Fiber-optic cabling and connectors are used to interconnect host bus adaptors, fibre channel switches and storage arrays

The Enterprise tier environment is managed with the following software:

Connectrix Manager	Client-server software that allows configuration and maintenance of the McData fibre channel switches.
Solutions Enabler	A collection of command line tools that allow configuration and maintenance of the Symmetrix storage arrays.

A simplified architecture of the enterprise tier SAN is illustrated in figure 1.

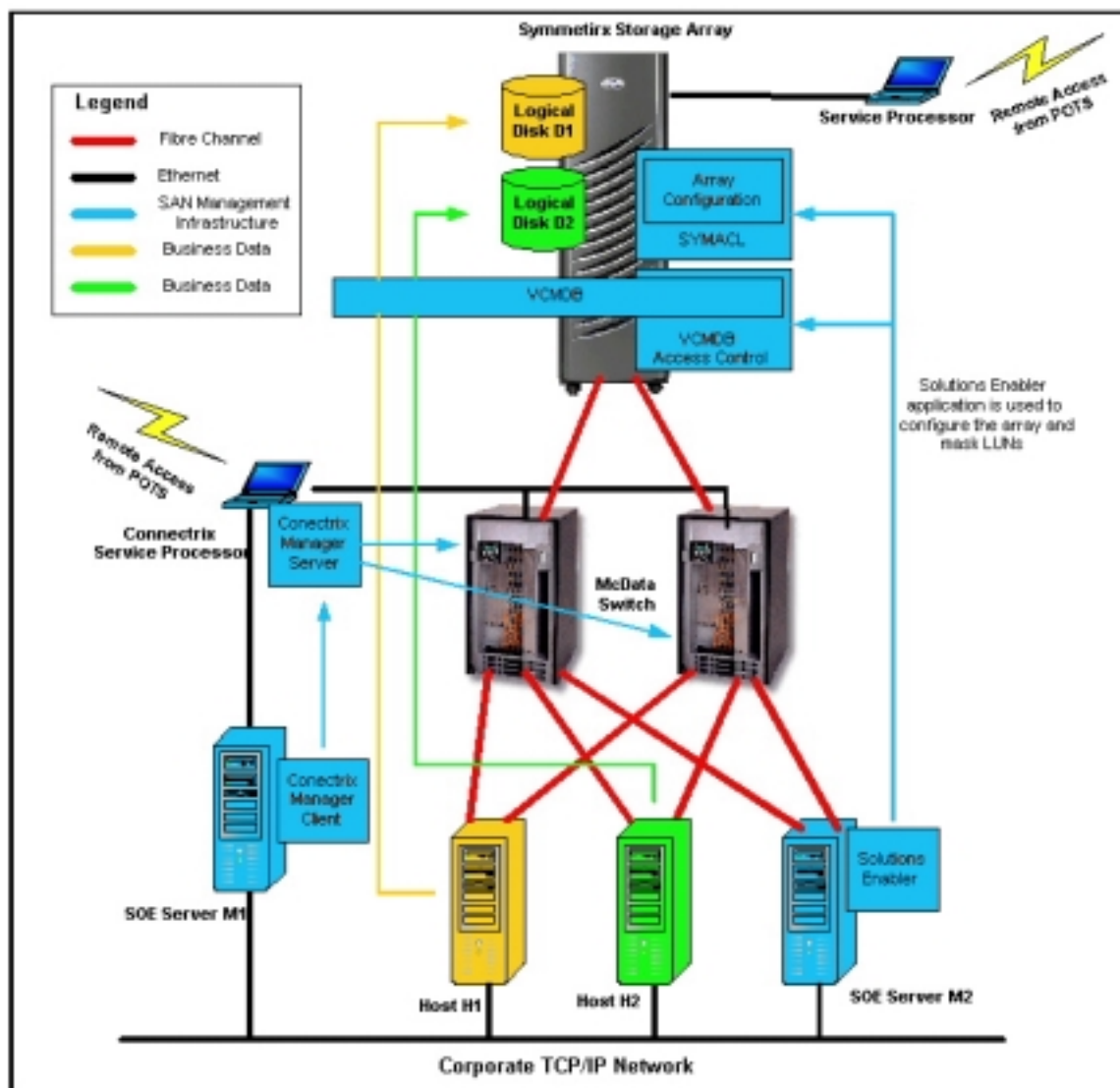


Figure 1 Enterprise Tier SAN

Hosts H1 and H2 are allocated disks D1 and D2 from the storage array over the fibre channel network. This allocation is controlled with the VCMDB database,

which can be updated by SOE Server M2 because it has permission in the VC MDB Access Control. The array configuration, such as disk layout, replication and business continuity volumes, can be controlled by SOE server M2, because it has been granted access in the SYMA CL database.

The vendor can initially set up the VC MDB Access Control and SYMA CL by using the service processor. Thereafter, the SOE Server M2 can manipulate these databases to grant access to VC MDB and array configuration to other hosts as needed.

The fibre channel network is made up of one or more McData fibre channel switches. The Connectrix Manager client is used from SOE server M1 to manage the switches. The client communicates with the Connectrix Service Processor running Connectrix Manager Server application, which in turn communicates with the switches. The Connectrix Manager application authenticates users, has role based access control and logs security and system administration events.

Both the Connectrix Service Processor and the Service Processor are remotely accessible over the public telephone network. The vendor uses this facility to be notified of faults and apply fixes from a remote location on a 24x7 basis.

8.1.2. Mid Tier SAN

The Mid Tier SAN solution offers the advantages of consolidated storage at a lower cost point. This solution is comprised of the following components:

EMC Clariion storage arrays	Provide highly available disk storage to hosts
Brocade or McData fibre channel switches	Provide highly available and scalable connectivity between the hosts and the array ports
Host Bus Adaptors	Enable hosts to connect to the Fibre Channel network
Interconnecting hardware	Fiber-optic cabling and connectors are used to interconnect host bus adaptors, fibre channel switches and storage arrays

The mid tier SAN environment is managed with the following software:

Brocade webtools or Connectrix manager	The Brocade FC switch is managed through a web interface known as “webtools”. The McData switches are managed with the Connectrix Manager application.
Navisphere	The Clariion array is managed by the GUI application called “Navisphere”
NaviCLI	The Clariion array can also be managed by command line tools

A simplified architecture of the Mid Tier SAN is illustrated in figure 2.

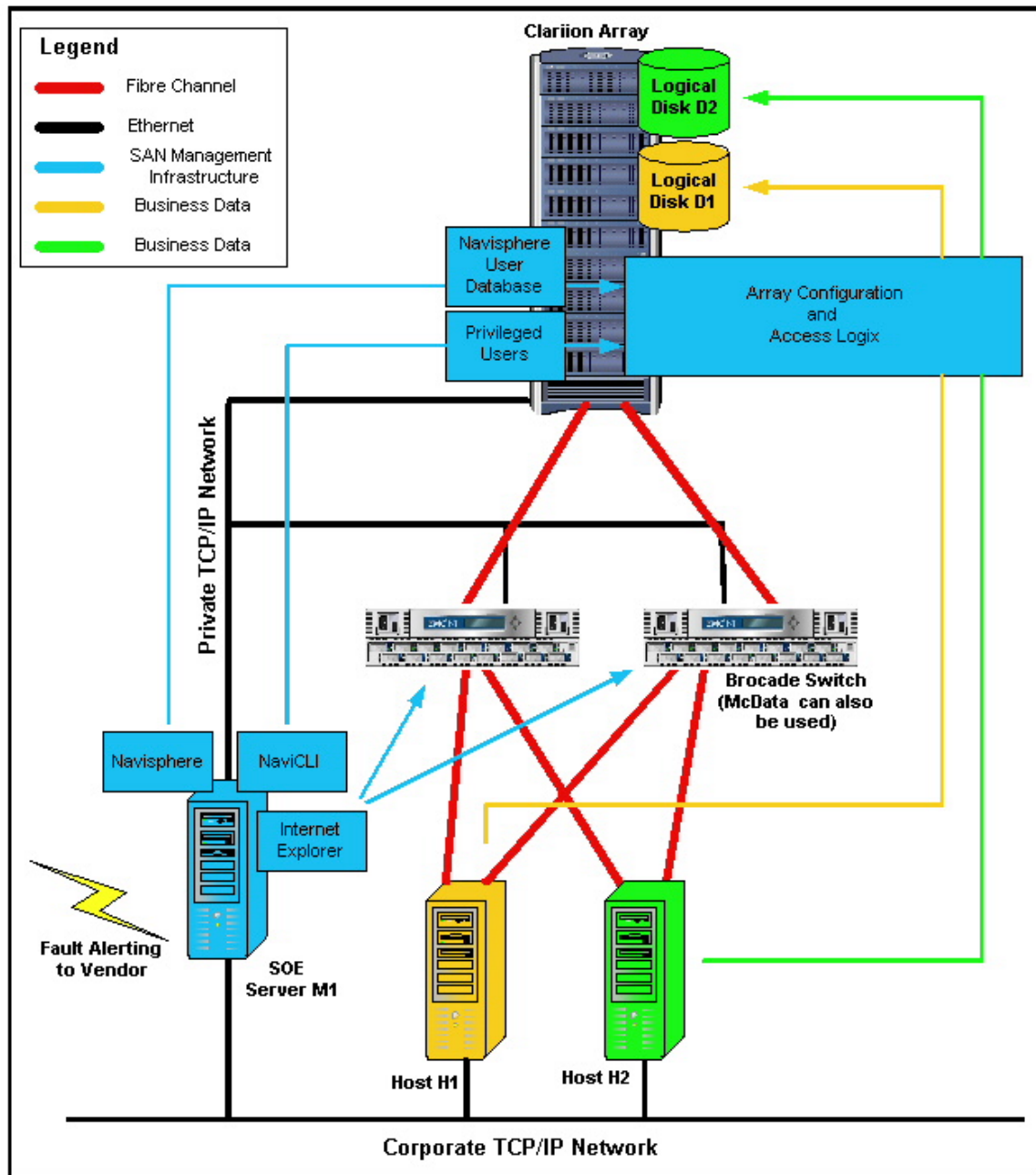


Figure 2 Mid Tier SAN

Hosts H1 and H2 are allocated disks D1 and D2 from the storage array over the fibre channel network. This allocation is controlled with the Access Logix product that is installed on the array. Privileged users can use the NaviCLI command line tools from the SOE server M1 to control Access Logix and the array configuration. Authorized users can also use the GUI application “Navisphere” from the SOE server M1 to control Access Logix and the array configuration. The

Internet Explorer browser on the SOE server M1 is used to manage the Brocade switches.

9. McData switch

9.1. Introduction

The McData switch provides highly available and scalable access to the SAN. It provides the following interfaces for access:

Access Protocol	Network Protocol	Remarks
CONSOLE	none	Serial console. Used for managing the switch. Requires physical access to the switch.
TELNET	TCP/IP	Used for managing the switch
HTTP	TCP/IP	Used for managing the switch
SNMP	TCP/IP	Used for managing the switch
NMRU	TCP/IP	Used by the Connectrix Manager application for managing the switch
OSMS	FC	Used for managing the switch
SWAPI	TCP/IP	Used for managing the switch
N_PORT	FC	Used by host to access the FC network
E_PORT	FC	Used to interconnect FC switches

9.2. Identification and authentication

The McData switch identifies devices connected to the N_PORT and the E_PORT with the World Wide Name ("WWN"). There is no authentication. To compensate, physical access to the switch should be controlled; the switch should be installed in a secure data center.

The switch can be managed with several interfaces. Some management interfaces, such as HTTP and TELNET, identify and authenticate users. Others, such as NMRU, do not identify users. To compensate for these weaknesses, the McData switch should only be managed with the Connectrix Manager application. The topology that enforces this is illustrated in figure 3.

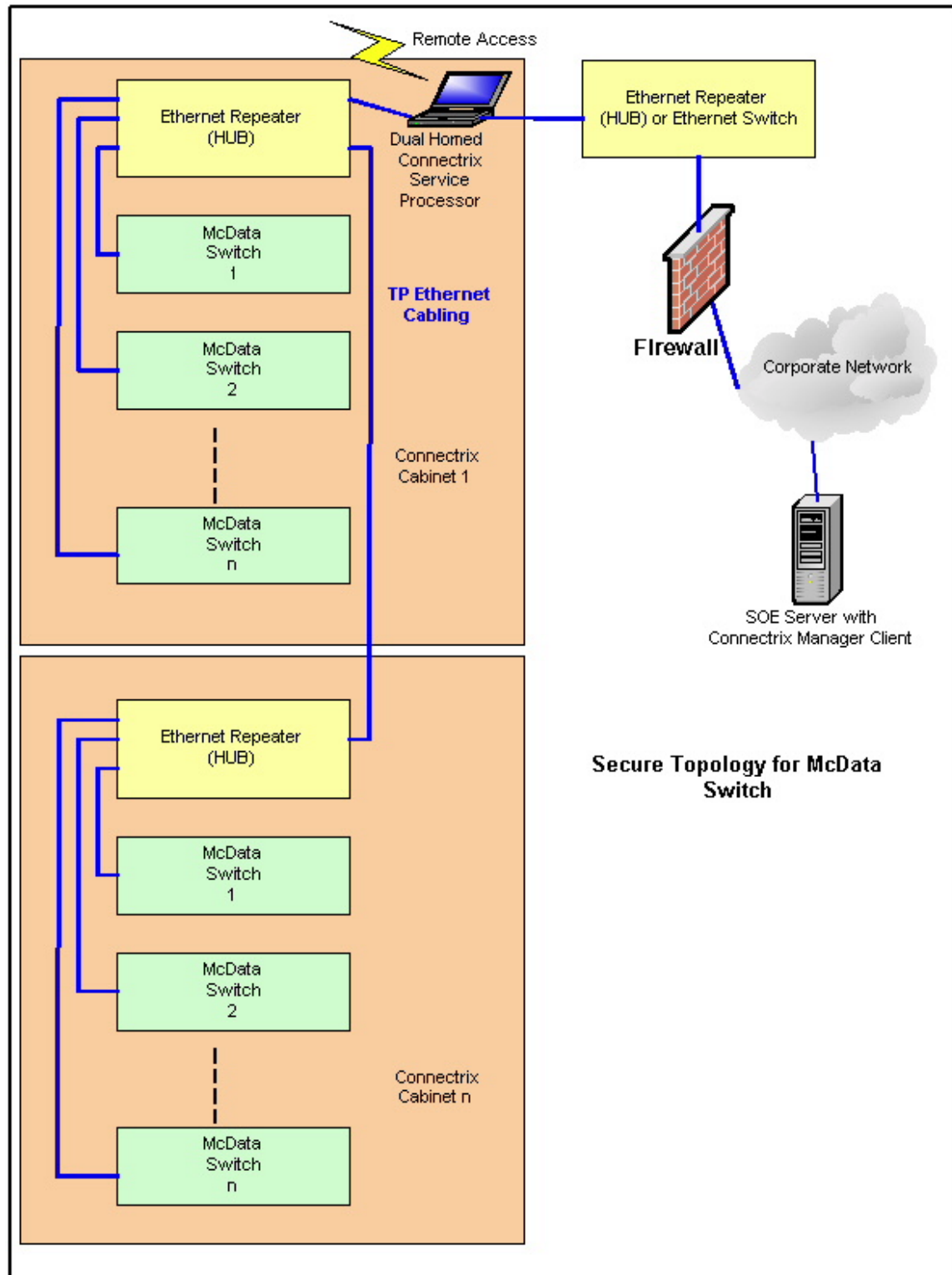


Figure 3 Secure Topology for McData Switch

The secure topology for the McData switch is illustrated in figure 3. In order to manage the switch, support staff would use the Connectrix Manager Client

application installed on the SOE server. The firewall protects the corporate network resources from the dial-in connection terminating on the Connectrix Service Processor (“CSP”), and protects the CSP’s weak controls from the corporate network.

9.3. Authorization and access control

The switch has the capability of controlling access to array ports based on the host identity, which is the WWN. Switch ports can be “zoned” to specific array ports. Several types of zoning are available, some more secure than others. Today, the company standard is to use WWN based zoning. Unfortunately, this type of zoning is designed to work in co-operation with the HBA driver. If the HBA driver so chooses, it can ignore the zoning configuration and communicate to unauthorized array ports, possibly gaining access to unauthorized disk resources.

The secure alternative to WWN zoning is “port zoning”. Although this technology is available on the installed base, it is not recommended since it has a large, negative impact on the storage provisioning process.

Because of the above weakness in the WWN zoning, it cannot be considered as a reliable control² for the purpose of this guide.

In the future, fibre channel switches will be able to enforce WWN zoning by actively inspecting and blocking fibre channel frames that do not meet the zoning criteria. Combined with a DH-CHAP based authentication for WWN, this technology is expected to provide a reliable access control mechanism at the switch level.

The lack of access control at the switch level is adequately compensated by the access controls on the storage array. These controls are discussed later in this document.

Access controls for the management of the switch are delegated to the Connectrix Manager application.

9.4. Confidentiality and Integrity

This component does not process³ or store business information. There are no configurable elements.

² WWN zoning should still be used as it resolves issues related to availability and serviceability of the SAN and provides additional, albeit insufficient controls over no zoning.

³ Even though business information passes through the switch, there is no interface for access

9.5. Incident detection and response

All logging is delegated to the Connectrix Manager application.

9.6. Administration

This component does not initiate, program, process, or authorize business transactions. This product does not internally support segregation of system and security administration or maker/checker functions.

The following default capabilities should be disabled or protected:

- From the product view within Connectrix Manager, disable the web server and telnet as shown in figure 4.

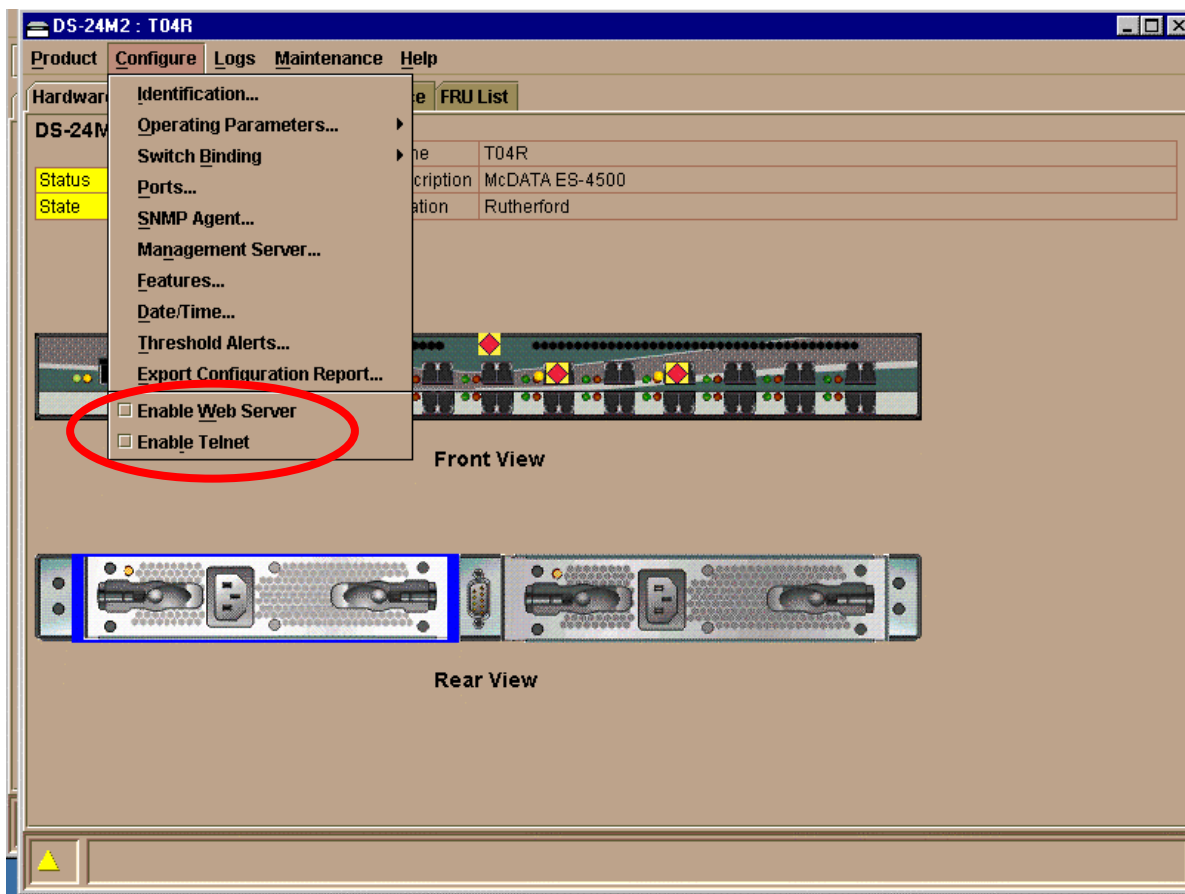


Figure 4 Disabling the Telnet and Web server on the McData switch

- From the product view within Connectrix manager, ensure that the SNMP agent on the switch does not permit writes. Please refer to figure 5. The SNMP agent is required to be configured with a read only “public” community string for use by the Connectrix Manager.

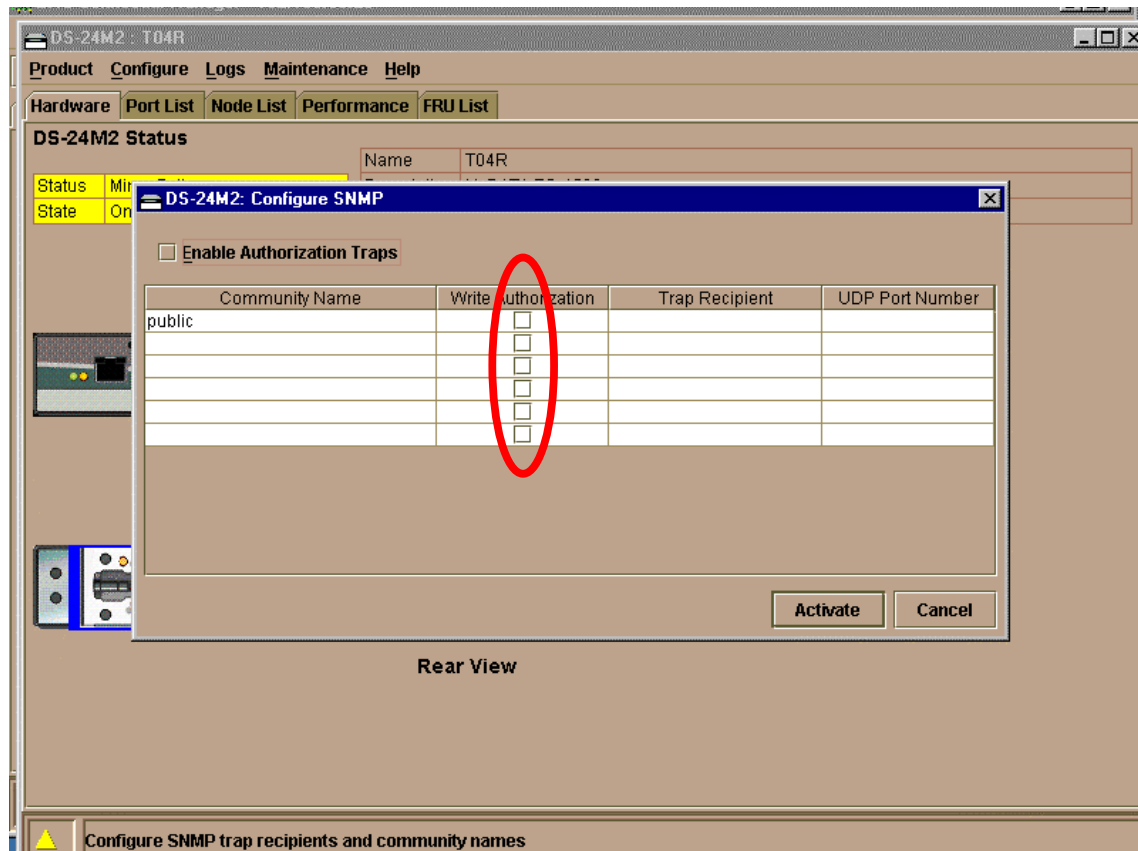


Figure 5 SNMP Agent configuration for the McData switch

9.7. Secure Fabric Configuration - SANtegrity

The SANtegrity product is a licensed enabled feature in Connectrix Manager for enhancing the security of the McData FC switches. In order to enable certain parts of SANtegrity (Fabric Bindings in phase I), a license string must be entered. To Enable the License key for the SANtegrity product, use the following steps:

- Go to the Hardware view in Connectrix Manager of the individual switch or switches that are being enabled. Use the Configure pull-down menu and select Features.
- Once the *Features* window is up, select *New* to add a new Feature. This will bring up the *New Feature Key* window so that the license key can be entered.
- After the Key has been entered, hit the *Ok* button.

- A new window will appear warning that the switch will IPL and have a momentary loss of LAN connectivity. Select the Yes button on the warning screen.
- At this point the switch may quit responding for a few seconds and the status may show link down but it will come back to operational.

Once this is done, the switch will have SANtegrity binding license enabled so that fabric and port bindings can be configured.

9.7.1 SANtegrity Port Bindings

For a secure SAN environment, Port bindings should be enabled and configured on all McData FC switches.

Port Bindings are designed to block unauthorized connections to the McData switches. When enabled, port binding authorizes a switch port to accept connections from only one designated WWN. If a different WWN is attached to the port, connectivity access will be denied. This eliminates the threat of obtaining unauthorized access to SAN resources by copying (“spoofing”) the WWPN from an authorized host. This also prevents failures related to accidental connection of devices to the wrong switch port (ie wrong fabric, incorrect cross fabric ISL).

To enable port bindings go to the Hardware view in Connectrix Manager of the individual switch that is being enabled. In order to enable port bindings, the following steps will be taken.

- Validate that all WWNs that are currently logged into the switch are valid.
- Validate that WWNs that are not currently logged into the switch that will (servers or storage that is down at the time bindings are enable) be enabled are valid.
- Bind all WWNs.
- Bind all ports to attached WWNs.
- Manually bind any WWNs of servers that may have been down when port bindings were enabled for the entire switch. (optional)

A manual validation must be done before port bindings are initially enabled to make sure that an invalid WWN is not granted permanent access to the SAN. The administrator should validate that all WWNs that will attach (from servers or storage that is down), and that are currently attached to the switch, are WWNs that come from known servers, storage, or switches. The administrator should also validate that there are no duplicate WWNs (spoofed WWNs).

After the WWN validation is done for a switch, the administrator then needs to bind all WWNs on the switch. To configure port bindings for all existing ports on the switch, the administrator needs to do the following:

- Go to the main *Products* view of Connectrix Manager and call up the individual switch that will get the port binding enabled.
- At the *hardware* view of the individual switch, hit the Configure pull-down menu and select Ports.
- On the *Configure Ports* window (shown below), *right click* in the *Port Binding* column for port 0 outside of the port binding check box and then select Bind All WWNs from the pull-down menu as shown below.

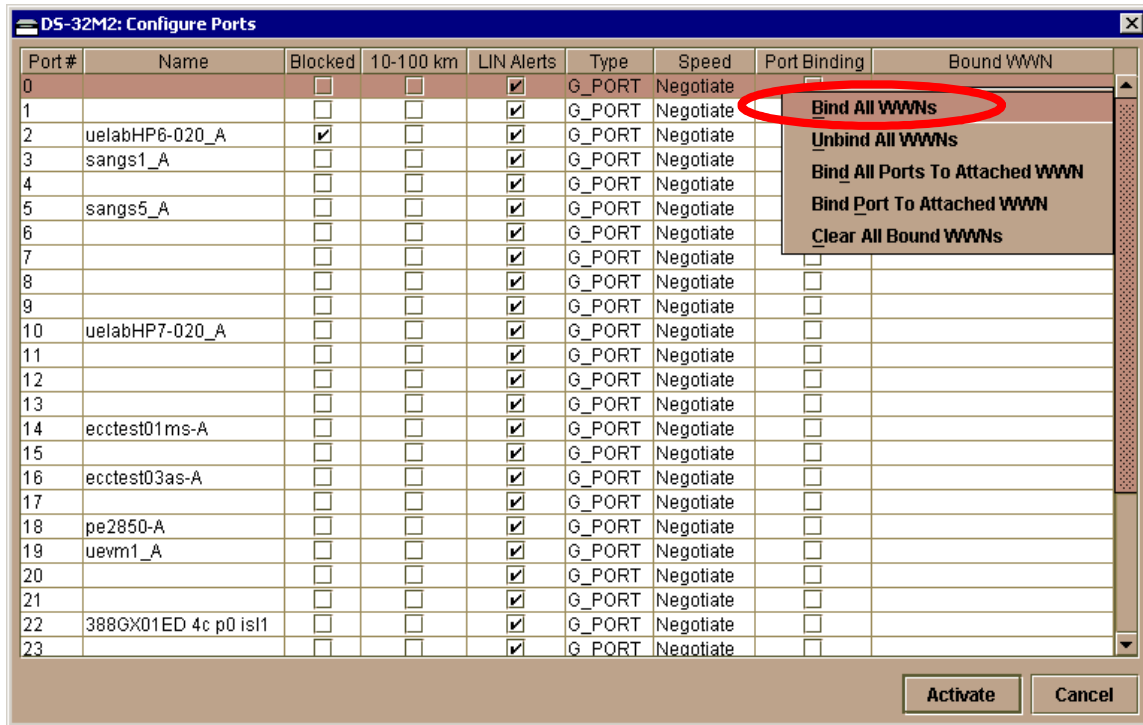


Figure 6 Bind All WWNs

- After the Bind All WWNs option has been selected, the check box for each port in the *Port Binding* column will now be checked as shown in figure 7 below.
- Now *right click* in the port 0 *Port Binding* column again and select Bind All Ports To Attached WWN from the pull-down menu.
- Now the *Bound WWN* column will have either a WWN or a WWN alias listed for all ports that have a fibre cable plugged in as shown in figure 7 below.
- If there is no cable plugged into a port, there will be nothing in the *Bound WWN* column as shown in figure 7 below.

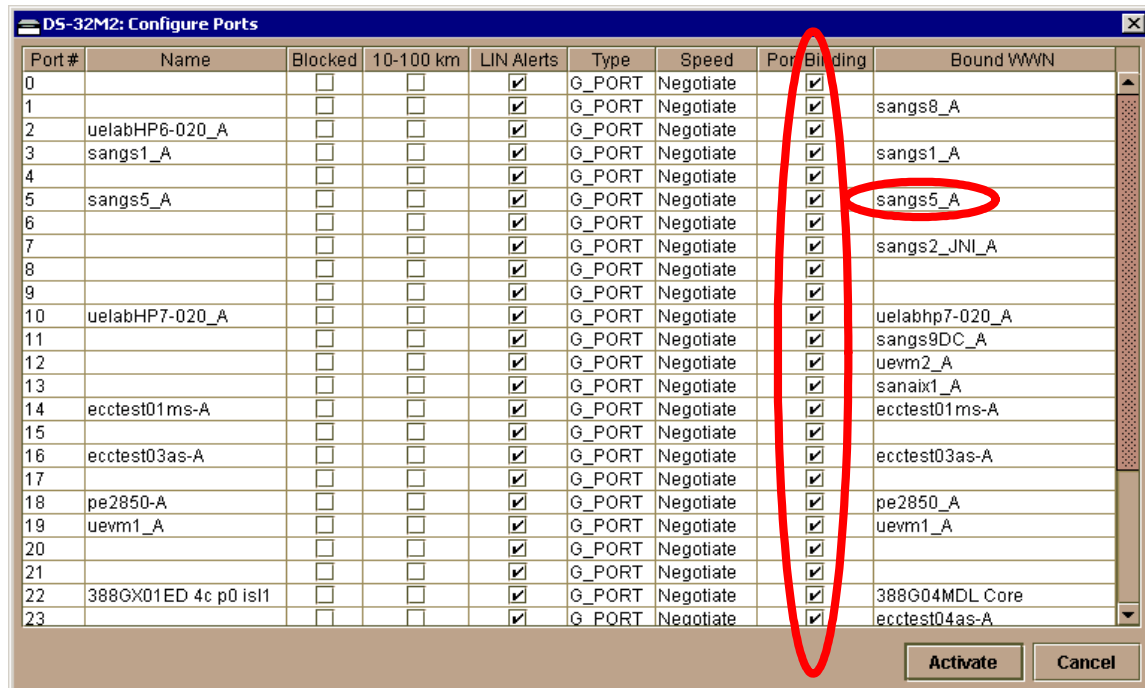


Figure 7 Bind All Ports To Attached WWNs

- At this point, press *Activate* and the bindings will take place and the *Configure Ports* screen will go away.

Now all ports that were logged in on the switch are bound to one of the following:

- A 64-bit WWPN (if no alias is assigned to the WWPN that is logged in)
- A WWPN Alias (if an alias is assigned to the WWPN that is logged in)
- NULL (if no cable is plugged into the switch port)
- A WWNN or WWNN Alias (if the port has an ISL plugged into it)

Even if the port has nothing plugged in, any attempt to plug in new cables without first unbinding the port will be denied. The port is bound to NULL, which will not match any WWPN that attempts to log into that port.

The administrator now needs to manually bind any server or storage that could have been down at the time the bindings were enabled. Failure to do this step would not allow any server or storage that was down during the time bindings were enabled to log into the SAN when they come back. The steps for doing this are as follows:

- Call the *Configure Ports* screen up again and go to the port that has a fibre cable plugged in that is not logged in because the server or storage is currently down, and was down during the Port Bindings.

- Manually enter the WWPN or the WWPN alias in the *Bound WWN* column and hit the activate button as shown in Figure 8 below.

Port #	Name	Blocked	10-100 km	LIN Alerts	Type	Speed	Port Binding	Bound WWN
0		☐	☐	☒	G_PORT	Negotiate	☒	
1		☐	☐	☒	G_PORT	Negotiate	☒	sangs8_A
2	uelabHP6-020_A	☐	☐	☒	G_PORT	Negotiate	☒	uelabhp6-020_A
3	sangs1_A	☐	☐	☒	G_PORT	Negotiate	☒	sangs1_A
4		☐	☐	☒	G_PORT	Negotiate	☒	
5	sangs5_A	☐	☐	☒	G_PORT	Negotiate	☒	sangs5_A
6		☐	☐	☒	G_PORT	Negotiate	☒	
7		☐	☐	☒	G_PORT	Negotiate	☒	sangs2_JNI_A
8		☐	☐	☒	G_PORT	Negotiate	☒	
9		☐	☐	☒	G_PORT	Negotiate	☒	
10	uelabHP7-020_A	☐	☐	☒	G_PORT	Negotiate	☒	uelabhp7-020_A
11		☐	☐	☒	G_PORT	Negotiate	☒	sangs9DC_A
12		☐	☐	☒	G_PORT	Negotiate	☒	uevm2_A
13		☐	☐	☒	G_PORT	Negotiate	☒	sanaix1_A
14	ecctest01ms-A	☐	☐	☒	G_PORT	Negotiate	☒	ecctest01ms-A
15		☐	☐	☒	G_PORT	Negotiate	☒	
16	ecctest03as-A	☐	☐	☒	G_PORT	Negotiate	☒	ecctest03as-A
17		☐	☐	☒	G_PORT	Negotiate	☒	
18	pe2850-A	☐	☐	☒	G_PORT	Negotiate	☒	pe2850_A
19	uevm1_A	☐	☐	☒	G_PORT	Negotiate	☒	uevm1_A
20		☐	☐	☒	G_PORT	Negotiate	☒	
21		☐	☐	☒	G_PORT	Negotiate	☒	
22	388GX01ED 4c p0 isl1	☐	☐	☒	G_PORT	Negotiate	☒	388G04MDL Core
23		☐	☐	☒	G_PORT	Negotiate	☒	ecctest04as-A

Figure 8 Manual Port Binding Entries

Now if this server were to come back online, the port would allow it to log into the SAN. If this step is not take, the port will have to be unbound and then rebound once the server comes backup before it will be allowed to log into the SAN.

9.7.2 SANtegrity Fabric Bindings

For a secure SAN environment, Fabric Bindings should be enabled and configured on all McData FC switches.

Fabric Bindings are designed to block unauthorized switches from joining an existing fabric via ISLs. Fabric bindings will also eliminate accidental fabric merges due to cabling errors. To enable Fabric Bindings, use the following steps:

- Go to the *Fabrics view* on the main Connectrix Manager window.
- Click a data point on the persisted fabric in the left hand column that is going to have fabric bindings enabled.
- Once the correct fabric shows up in the *Topology view*, select the *Fabrics* pull-down menu and select *Fabric Bindings*.
- When the *Fabric Binding* window appears, check the *Enable Fabric Binding* check box and then hit *Next*.

- At this point a *Fabric Binding Membership List* window will come up. On the *Membership List* window all of the switches in the selected fabric should be contained in the list, if they are not then add them to the membership list as shown in figure 8.

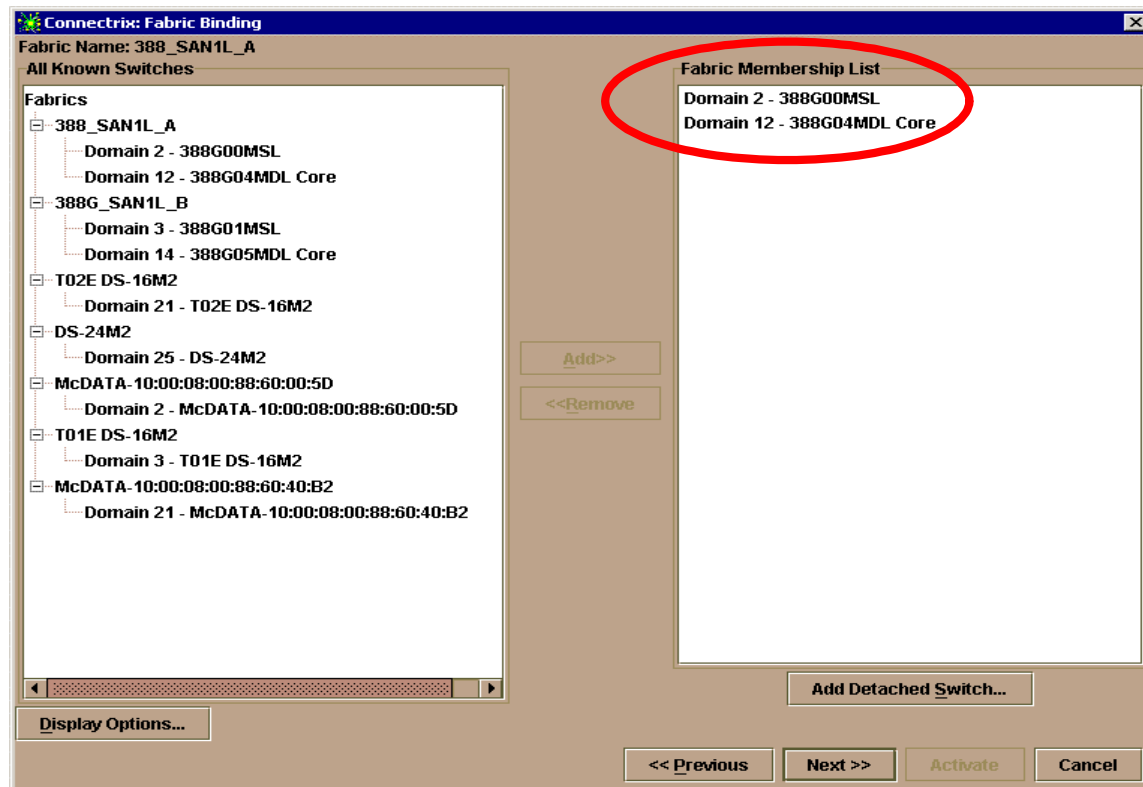


Figure 9 Fabric Membership List

- Hit *Next>>* on this window and a summary screen will then appear showing the fabric membership list and that the *Fabric Binding Activation setting* is set to Enable⁴.
- At this screen hit the *Activate* button and the *Fabric Binding Activation Progress* screen will appear.
- Once the progress shows complete, hit the *Close* button and the fabric will be bound.

This process needs to be repeated for each fabric (multi or single switch) on the Connectrix Manager *Fabric View*.

⁴ Because switches are bound by WWN and domain ID, the Insistent Domain ID option in the Configure Switch Parameters dialog box is automatically enabled when you enable fabric bindings. You cannot disable Insistent Domain ID while fabric binding is enabled.

9.8. SANtegrity Operational Changes

Once SANtegrity bindings are implemented at the port and fabric level, the normal Operations procedures for plugging new connections into the switch will change. The following sections will list and document these operational changes.

9.8.1 Adding New Storage/Server Connections to the Switch

Prior to SANtegrity when an administrator wanted to plug new storage or server connections into the SAN, the administrator only needed to plug the new cables into the SAN and let the connection login. With port bindings enabled, if an administrator were to try and do this on an empty port, the connection would not login, and the port properties would show that there are binding errors as show below.

Port Number	2
Port Name	uelabHP6-020_A
Type	G_Port
Operating Speed	2 Gb/sec
Fibre Channel Address	000000
Port WWN	McDATA-20:06:08:00:88:A0:D6:62
Attached Port WWN	Not logged in
Block Configuration	Unblocked
10-100 km Configuration	Off
LIN Alerts Configuration	On
Beaconing	Off
Link Incident	None
Operational State	Invalid Attachment
Reason	10: Port binding violation - unauthorized WWN
Threshold Alert	

The new process for plugging a new server or storage fibre cable into the SAN will be as follows.

- Call up the *hardware view* of the switch, and select the Configure pull-down menu and then select Ports.
- Unbind the empty port by clearing the check box in the *Port Binding* column of the port in question, and then manually clearing any entry (if one exists) in the *Bound WWN* column, and then hit the *Activate* button.
- Plug the new server or storage cable into the Port. With the bindings for that port turned off the connection should now log into the fabric.
- Manually validate the logged in WWN matches what is expected.
- Then *right click* in the *Port Binding column* for the port and select *Bind Port to Attached WWN* from the pull down menu, then hit the *Activate* button. This will only bind the port in question.

9.8.2 Adding New Switches to the Fabric

The process of adding a new switch to an existing fabric will change with the additions of fabric bindings. Without fabric bindings, storage administrators only needed to add a new ISL from the new switch to the existing fabric, let the fabric rebuild, and then re-persist the fabric. If an administrator were to try this approach with Fabric and Port bindings enabled, the fabric would not merge and the ISL port would show a link alert with *Incompatible security attributes* for the *Reason* in the port properties as shown below.

Port Number	62
Port Name	
Type	G_Port
Operating Speed	2 Gb/sec
Fibre Channel Address	000000
Port WWN	McDATA-20:42:08:00:88:A0:4C:8A
Attached Port WWN	Not logged in
Block Configuration	Unblocked
10-100 km Configuration	Off
LIN Alerts Configuration	On
Beaconing	Off
Link Incident	None
Operational State	Invalid Attachment
Reason	12: Incompatible security attributes
Threshold Alert	

Close

The correct order for adding a new switch into an existing fabric with fabric and port bindings enabled is as follows.

- Add the new switch as a new managed object into the Connectrix Manager main view.
- Unbind the empty port on both the new and existing switch that will hold the ISL by clearing the check box in the *Port Binding* column on the *Configure Ports* screen, and clearing any entry in the *Bound WWN* Column.
- Call up the fabric bindings for the existing fabric where the new switch will be added and add the new switch into the fabric membership list.
- The new switch should still show up as it's own fabric in the fabric view at this point. Highlight the new switch in the fabric view and enable fabric bindings on the new switch. Add all existing switches to the fabric membership list from the fabric that the new switch will join and enable fabric binding.
- After the new switch is added into the existing fabric membership list and the new switch contains all switches in it's fabric membership list that it will join, the administrator can now plug the new ISLs in and the fabric will merge with the new switch in the fabric.

- On both the new switch and the existing switch that holds the ISL from the new switch, a *Bind Port to Attached WWN* must be done on the ISL ports.
- Re-persist the fabric that should now include the new switch.

9.8.3 Adding Additional ISLs from Existing Switches

Adding an additional ISL from existing switches in a fabric would follow the same rules as adding new storage or server connections to the SAN except that the fabric would need to be re-persisted once the change is made. Adding a new ISL would not require any changes to the fabric bindings since the existing switches WWNs and Domain IDs would already be in the fabric membership lists. The steps would be as follows.

- Unbind the empty ports on each existing switch that will hold the new ISL by clearing the check box in the *Port Binding* column, and clearing any entries in the *Bound WWN* column.
- Plug the new ISL cable into the Ports on each switch. With the bindings for the ports turned off on both switches the connection should log into the fabric, and the fabric should rebuild.
- Then *Bind Port to Attached WWN* from the Port Bindings screen on each switch port that holds the new ISL. Bind only the port in question on each switch.
- Re-persist the fabric.

9.8.4 Removing Hosts from Switches

The procedure for removing a server from the SAN will change to include the port bindings functionality. Prior to SANtegrity, an administrator only needed to unplug a server from the SAN that would no longer require SAN connectivity. Due to the implementation of port bindings, the new procedure for removing servers from the SAN is as follows:

- Unbind the ports on each existing switch that currently hold the server to be removed by clearing the check box in the *Port Binding* column, and clearing any entries in the *Bound WWN* column.
- Remove the server's fibre cable from the switch.
- Bind the switch port to nothing/NULL by checking the binding check box for the now empty port.

9.8.5 Removing ISLs from Switches

The following steps will explain how to remove an ISL from a switch that has multiple ISLs to the same location. If a source switch has multiple ISLs to a target switch and one needs to be removed, the fabric bindings will not come into play since the switch domain ID and WWN will still exist in the fabric membership list because of the ISLs that will not be removed.

Removing one of multiple ISLs to a target switch will only impact port bindings. To remove an ISL from a source switch that has multiple ISLs going to the same target switch follow these steps:

- Unbind the ports on each existing switch that currently hold the ISL that will be removed by clearing the check box in the *Port Binding* column, and clearing any entries in the *Bound WWN* column.
- Unplug the ISL cable on both the source and target switches. At this point the fabric should rebuild.
- Bind the now empty ports that held the ISL on both the source and target switches to nothing/NULL.
- Re-persist the fabric so that the fabric topology will be updated.

9.8.6 Removing Switches from a Fabric

The new process for removing a switch from a fabric will involve changes both in the Fabric and Port binding configurations. The new process for removing a switch from the fabric will be as follows:

- Unbind the ports on each existing switch that currently hold the ISL/ISLs that will be removed by clearing the check box in the *Port Binding* column, and clearing any entries in the *Bound WWN* column.
- Unplug the ISL/ISLs cable from both the associated switches. The fabric will rebuild at this point.
- Remove the switch from the fabric membership list in the Fabric Bindings for the fabric where the switch will be removed.
- Re-persist the fabric to update the topology for the fabric.
- Bind the now empty ports that held the ISL to nothing/NULL.
- On the switch that was removed, disable fabric bindings.

10. Connectrix Manager

10.1. Introduction

The Connectrix Manager is a client-server application that is used to manage the McData switches. The Connectrix Manager server component is installed on a vendor controlled, non-SOE hardware called the Connectrix Service Processor ("CSP"). The Connectrix Manager server communicates with the McData switches by using the NMRU protocol over TCP/IP. The Connectrix Manager client component is installed on a SOE server, and communicates with the Connectrix Manager server by using the RPC protocol over TCP/IP.

10.2. Identification and authentication

The Connectrix Manager application identifies and authenticates users. The application maintains its own user and password database. A built-in “Administrator” ID is provided, which should not be used by the support staff for day-to-day needs. The password for the “Administrator” ID should be secured.

The SAN IS product TRAM documents several gaps in the Connectrix Manager product. To compensate for these gaps, the Connectrix Manager client application should be installed on a SOE server, so that users first identify and authenticate to the SOE server. This is enabled by the topology illustrated in figure 3.

Further, Storage Management should create level 3 procedures to ensure that passwords are six or more alphanumeric characters, passwords are changed periodically, inactive user accounts are removed and user accounts for users that are no longer responsible for support are removed.

10.3. Authorization and access control

The Connectrix Manager application offers role based access control. A list of roles and associated privileges is listed in appendix C.

The logon on the SOE server hosting the Connectrix Manager client should be limited to support staff authorized by Storage Management.

Storage Management should carry out periodic review of the above user entitlements.

10.4. Confidentiality and Integrity

This component does not process or store business information. There are no configurable elements.

10.5. Incident detection and response

The Connectrix Manager application is capable of logging system and security events as illustrated in appendix D. These logs should be archived, and should be periodically reviewed.

10.6. Administration

This component does not initiate, program, process, or authorize business transactions. This product does not internally support segregation of system and security administration or maker/checker functions.

The following default capabilities should be disabled or protected:

- The default password for the built in “Administrator” user ID should be changed at the time of install⁵
- SNMP should be turned off by clearing the “Enable SNMP agent on server” checkbox as shown in figure 6.

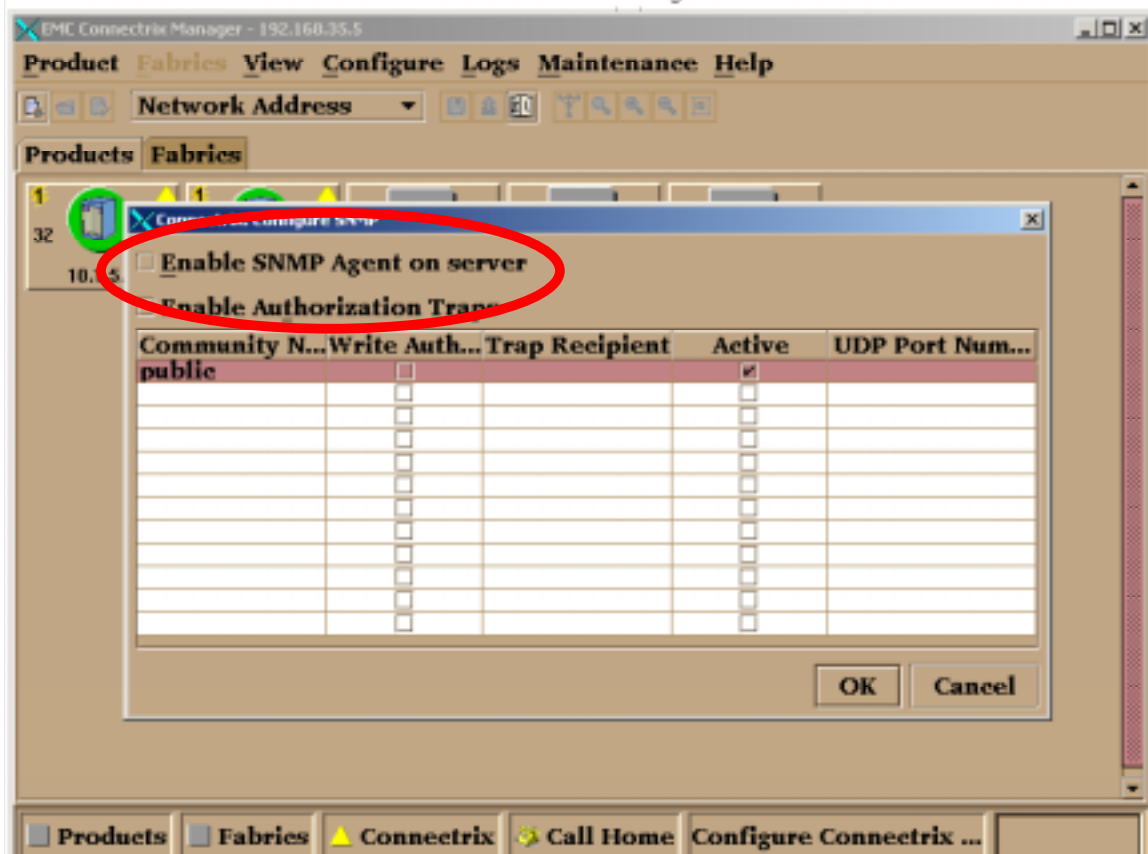


Figure 10 Disabling the SNMP Agent on Connectrix Manager

- In case the SNMP agent has to be enabled, community string should be at least 6 characters with alpha and numeric characters, and write authorization should be turned off. This is illustrated in figure 7.

⁵ The Connectrix Manager user and password database is stored on the Connectrix Service Processor. Any Connectrix Manager client instance can be used to change the password.

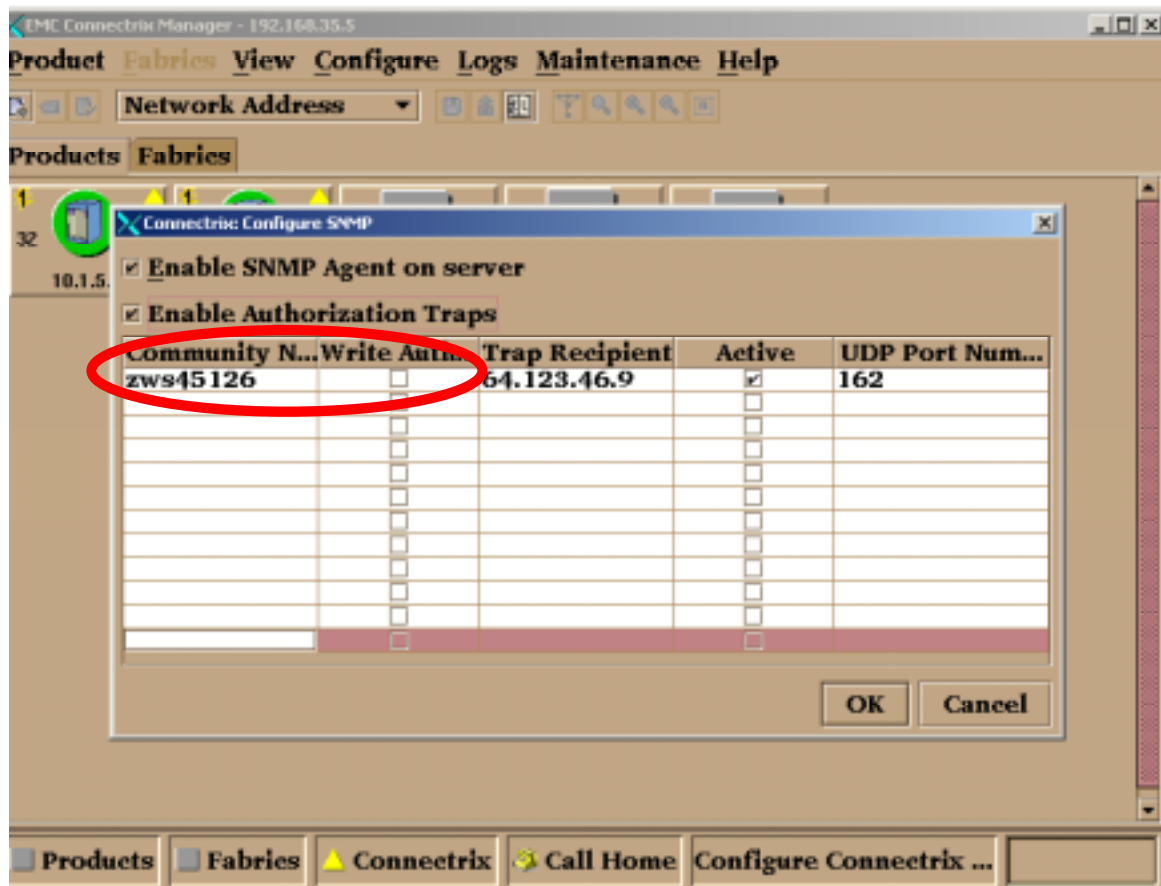


Figure 7 Enabling the SNMP Agent on Connectrix Manager

- Connections to the Connectrix Manager server should be limited to hosts that are authorized by Storage Management. Such servers would include any SOE server(s) hosting the Connectrix Manager client. The restriction can be enabled from the Configure -> Sessions menu, as illustrated in figure 8.

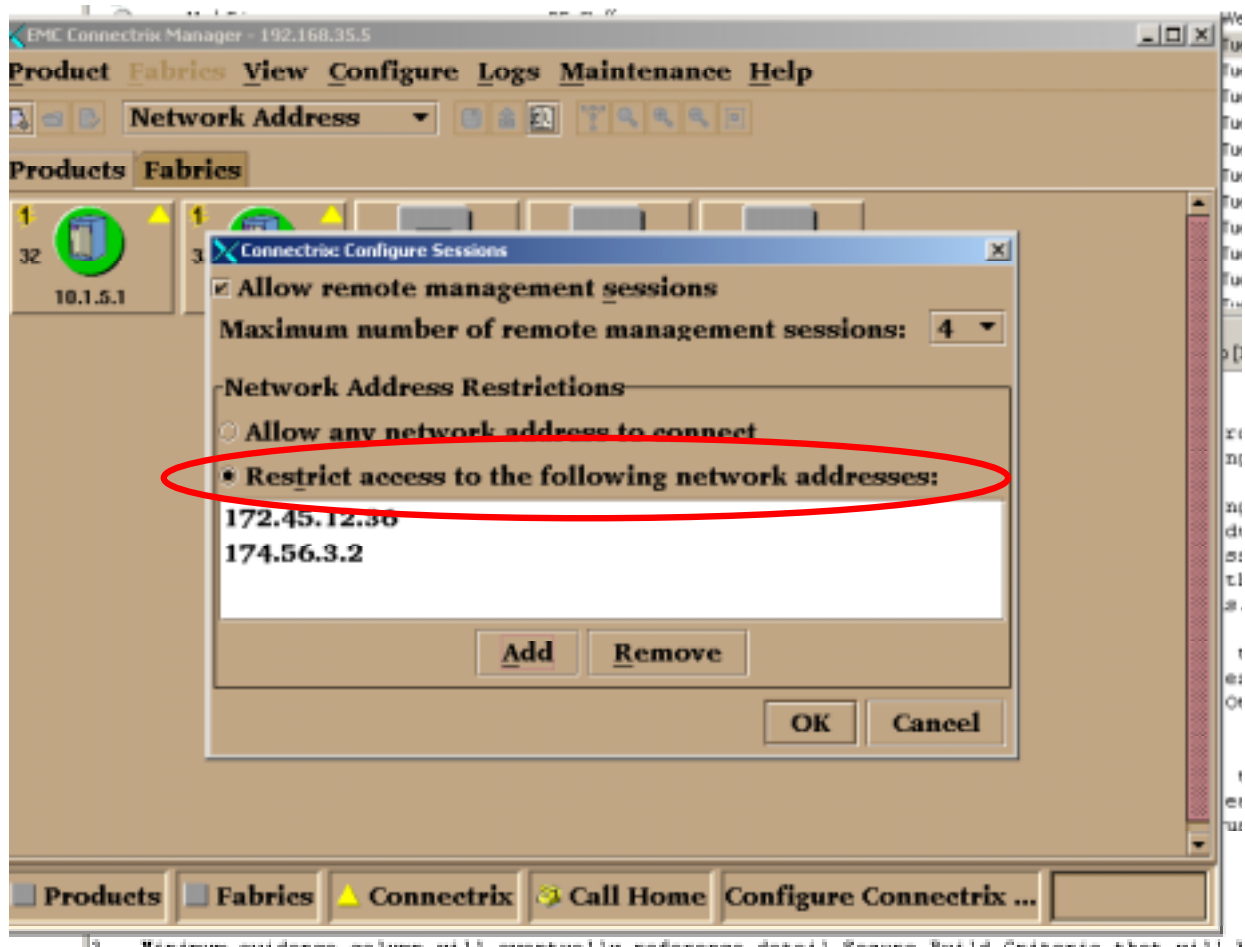


Figure 11 Restricting Access to Connectrix Manager

- The logons on the SOE server hosting the Connectrix Manager client should be limited to personnel authorized by Storage Management.

11. Symmetrix Array

11.1. Introduction

The Symmetrix Array offers block access storage to hosts over the FC network using the SCSI protocol. The Symmetrix arrays can be managed in-band, via the fibre channel network, or out-of-band, via the TCP/IP interface. The Service Processor within the array allows vendor personnel to carry out initialization, advanced configuration and diagnostics on-site or from a remote support center.

Access Protocol	Network Protocol	Remarks
PROPRIETARY (GATEKEEPER)	FC/SCSI	Used for managing the array
PROPRIETARY (VCMDB)	FC/SCSI	Used for managing access control lists that control host access to storage
SCSI	FC	Used by hosts to access storage
PROPRIETARY (from Service Processor)	TCP/IP	Used by the Service Processor for managing the array

11.2. Identification and authentication

The array identifies hosts by their World Wide Name ("WWN"). The array does not authenticate the identity of the hosts. To compensate, the fibre channel network that provides access to the array must not expand beyond a secure data center.

Because the identification and authentication mechanisms on the TCP/IP interface are unknown, it should not be connected to a private or public TCP/IP network. Instead, all management tasks should be carried out in-band, through the fibre channel network.

11.3. Authorization and access control

The array offers the following three controls:

1. Access to storage within the array - VCMDB
2. Access to entries within the VCMDB - VCMDB Access Control
3. Access to array configuration - SYMACL

To enable these controls, the array must be configured as follows:

- SYMACL should be turned on at the time of install.
- Use SYMACL to restrict SYMCLI access to only those hosts that have been authorized by Storage Management.
- VCMDB Access Control should be turned on at the time of installation.
- Use VCMDB Access control to restrict VCMDB access to only those hosts that have been authorized by Storage Management

Periodic entitlement reviews must be conducted for the above controls.

The following sections detail the configuration with VCMDB access control and SYMACL.

11.3.1. Volume Control Masking Database (VCMDB)-Host/HBA Restriction

Standard practice for EMC Symmetrix/DMX bin file configurations is to present LUN0 to all front-end fibre adapters (FA's). This configuration allows storage administrators the ability to use any FA port for access to the VCMDB device for device masking operations. In the past, this practice was also used to provision LUN0 to every host in order to update the VCM database with the host name using the "vcfind" utility. Unfortunately, this very configuration enables any SAN attached host to possibly access the VCMDB, and perform device-masking operations.

The Symmetrix has a defined set of Symmetrix-Wide configuration metrics that include the following:

max_hypers_per_disk
dynamic_rdf
FBA_multi_access_cache
raid_s_support
VCMDB_restricted_access
raid_s_members
raid_5_support

For the purpose of this section, however, we will focus on the "VCMDB_restricted_access" metric.

"VCMDB_restricted_access" - enables you to restrict access to the device-masking database to hosts that have a database entry that includes the VCMDB device. By default, all Host Bus Adapters (HBAs) that log in to the FA port to which the VCMDB device is mapped can access the database. By setting this parameter value to ENABLE, access to the VCM database is denied to all hosts except those who's HBAs have been added the VCMDB device through the "*symmask add devs*" command.

The Configuration Manager "symconfigure" functionality included in Solutions Enabler version 5.2.0.13 or higher is required to enable "VCMDB_restricted_access" on Symmetrix/DMX with the following Enginuity code versions:

5567.53.30 - GDSE Certified

5568.56.22 - GDSE Certified

5670.73.69 - GDSE Certified

Failure to use these Certified versions may result in serious side effects. SAN administrators should have strong knowledge in the use of SYMCLI "symconfigure" command before running any symconfigure command.

Before enabling the "VCMDB_restricted_access" metric the storage administrator must "symmask add devs" Symmetrix device 0000 to at least **two** HBAs from the SAN management host (SANADx). **Only** HBAs masked to device 0000 will have access to VCMDB control functions and the VCMDB device. If required, additional host HBAs can be given access to the VCMDB device from the SAN Management host.

Should access to the VCMDB be lost from the SAN Management host(s), the local EMC CE has the capability to disable "VCM_restricted_access" from the Symmetrix/DMX service processor.

NOTE: you can list all host(s) HBAs that have been mask(ed) to the VCMDB device with the following command:

"symmaskdb -sid xxxx list assignments -dev 0000".

11.3.1.1. "VCMDB_restricted_access" Configuration and Setup

Configuration of "VCMDB_restricted_access" requires the following detailed procedures:

- 1) From the SAN Management control workstation, ensure the correct version of SYMCLI and Symmetrix Microcode are installed.
 - a) Run "symconfigure -sid xxxx list -v" (figure 8)



```

Select C:\WINNT\System32\cmd.exe - what args?
bash-2.01B symconfigure -sid 0128 list -v

Symmetrix ID : 000007430120
Configuration Server Version : 5570.73.69
Configuration Server Protocol : 86400
Configuration Server Date : 05.13.2004

F00 formatted : 200004
F00 unformatted : 0
4E/400 formatted : 0
4E/400 unformatted : 0
100_F00 formatted : 0
100_F00 unformatted : 0
0M1005_F00 formatted : 0
0M1005_F00 unformatted : 0
100 formatted : 0
100 unformatted : 0
000-1000 formatted : 0
000-1000 unformatted : 0
000-1000 formatted : 0
000-1000 unformatted : 0

Max Bytes per Disk : 16
F00 Multi Access Cache : Enabled
Dynamic RRP Configuration : Disabled
R010-S support : Disabled
R010-S numbers : 2
VCMDB Access Restricted : Enabled

bash-2.01B _
  
```

Figure 12 - EMC Symmetrix detailed version information

b) Run “symcfg –sid xxxx list –v” (figure 9)



```

C:\WINNT\system32\cmd.exe - telnet sangs7
bash-2.03# symcfg -sid 0120 list -v
Symmetrix ID: 000387430120

Product Model           : 1000S-M2
Symmetrix ID            : 000387430120

Microcode Version (Number) : 5670 (16260000)
Microcode Date           : 05.13.2004

Microcode Patch Date      : 05.13.2004
Microcode Patch Level     : 73

Cache Size               : 16384 (MB)
# of Available Cache Slots : 315967
# of PermaCache Slots In Use : 36072
Max # of System Write Pending Slots : 253020
Max # of DA Write Pending Slots : 126510
Max # of Device Write Pending Slots : 3615

Symmetrix Total Operating Time : 39 days, 23:21:36
Symmetrix Power ON Time       : Wed Jun 30 12:18:55 2004
Symmetrix Last IPL Time (Cold) : Wed Jun 30 12:20:35 2004
Symmetrix Last Fast IPL Time (Hot) : Thu Jul 29 10:40:19 2004

Host DB Sync Time          : Thu Aug 5 15:55:50 2004
Symmetrix CLI (SYMCLI) Version : 05.2.0.13 (Edit Level: 425)
Built with SYMAPI Version    : 05.2.0.13 (Edit Level: 425)
SYMAPI Run Time Version     : 05.2.0.13 (Edit Level: 425)

Number of Configured (Syn) Devices : 1075
Number of Visible (Host) Devices : 26
Number of Configured Actual Disks : 98
Number of Configured Hot Spares : 0
Number of Unconfigured Disks : 0
Maximum number of hypers per disk : 16

Number of Powerpath Devices : 8
Powerpath Run Time Version : 4.1.0

SDDF Configuration State : Enabled
Configuration Change State : Enabled
WORM Configuration Level : N/A
WORM Characteristics : N/A

Symmetrix Configuration Checksum : 31D019
Switched RDF Configuration State : Enabled
Concurrent RDF Configuration State : Enabled
Dynamic RDF Configuration State : Disabled
RDF Data Mobility Configuration State : Disabled
Access Control Configuration State : Enabled
Device Masking (UCM) Config State : Enabled
UCMdb Access Restricted State : Enabled
Multi LRU Device Assignment : BY_NUMBER

Parity Raid Configuration : N/A

bash-2.03#

```

Figure 13 - EMC Solutions Enabler detailed version information

1) Check the symapi_licenses.dat file to ensure the Configuration Manager license is installed. If it is not, consult your EMC CE or Account Manager for the “ConfigChnge” license key.

a) For Win2K SANAD servers: (figure 10)

i) Change directory \Program Files\EMC\SYMAPI\config\

- ii) Read the "symapi_licenses.dat" file
- b) For Solaris SANAD servers:
 - i) Change directory \var\symapi\config\
 - ii) Read the "symapi_licenses.dat" file

NOTE: if the "ConfigChange / Symmetrix" license is not installed then perform step C.

- c) If license not installed:
 - i) Run "symlmf" command
 - ii) Add license key per instructions (figure 10)

```

C:\WINNT\System32\cmd.exe
10/31/2003 01:12p <DIR> -
10/31/2003 01:12p <DIR> -
10/31/2003 01:04p 1,483 clarcnfg
11/03/2003 03:25p 2,298 netcnfg
10/31/2003 01:04p 9,293 options
10/31/2003 01:04p 1,483 README.clarcnfg
10/31/2003 01:04p 2,193 README.netcnfg
10/31/2003 01:04p 9,293 README-options
10/31/2003 01:04p 717 symapiinlck
10/31/2003 01:08p 0 symapislck
11/03/2003 12:56p 433 symapi_licenses.dat
9 File(s) 27,193 bytes
2 Dir(s) 4,599,185,408 bytes free

C:\Program Files\EMC\SYMAPI\config>more symapi_licenses.dat
License Key: 7FBE-9150-E0BC-9CCD WIDESKY Feature: BASE / Symmetrix
License Key: 3A61-6044-C190-0196 WIDESKY Feature: SERVER / Symmetrix
License Key: C7B7-B992-1954-4D99 WIDESKY Feature: DeltaMark / Symmetrix
License Key: A97E-6602-DABA-9E2A WIDESKY Feature: DevMasking / Symmetrix
License Key: 8EC5-F23C-F234-F081 WIDESKY Feature: SRDF / Symmetrix
License Key: 4B00-4011-EF38-1609 WIDESKY Feature: TimeFinder / Symmetrix

C:\Program Files\EMC\SYMAPI\config>symlmf

      E M C      W I D E S K Y

      WIDESKY LICENSE MANAGEMENT FACILITY

Register WIDESKY License Key <y/In> ? y
Enter WIDESKY License Key : A936-39CD-A0FF-CDC5

Register WIDESKY License Key <y/In> ? n
C:\Program Files\EMC\SYMAPI\config>
  
```

Figure 14 - Solutions Enabler "symlmf" utility

NOTE: The SAN Management host should have the EMC Solutions Enabler software already installed with, at minimum, the following licenses:

BASE / Symmetrix
 SERVER / Symmetrix
 DevMasking / Symmetrix

To create or change configuration information in the Symmetrix/DMX database, you need to enter the changes in a command file and eventually commit the file. The command file format can contain various command entries terminated with a semicolon (;). The command syntax is parsed case insensitive, but any variable parameter entered must be case sensitive.

- 2) Following the procedures for using "symconfigure", create and execute the command file (for example; restrictvcm.cmd) with the metric parameters

written in the file. The command file is used to present configuration change requests to the Symmetrix unit.

- a) Using your favorite text editor, create a text file using the “.cmd” extension:
 - i) “edit restrictvcm.cmd”
- b) Write the following metric parameter:
 - i) “set SYMMETRIX VCMDB_restricted_access=enable;”
note semi-colon(;) at end of line. (figure 11)
- c) Save file.

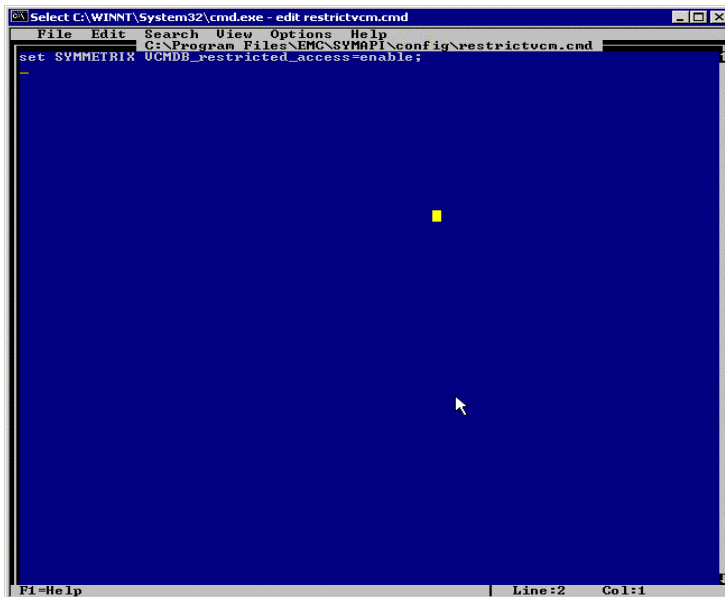


Figure 15 - VCMDB_restricted_access command file

- d) Verify HBAs assigned to VCMDB device. (figure 12)
 - i) Run “symmaskdb -sid xxxx list assignment –dev 0000”

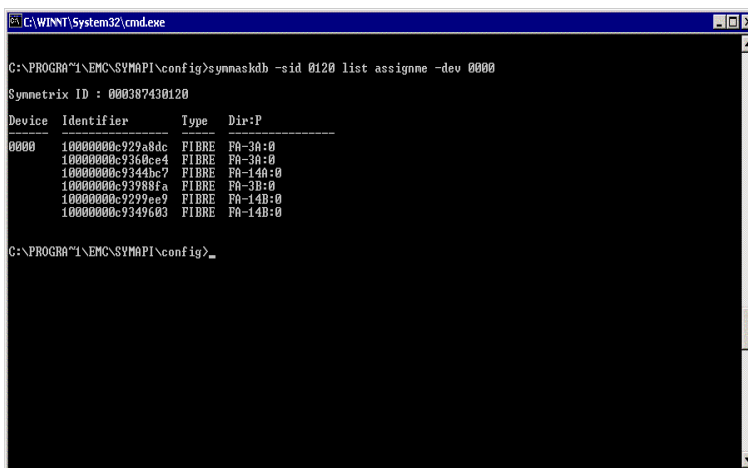


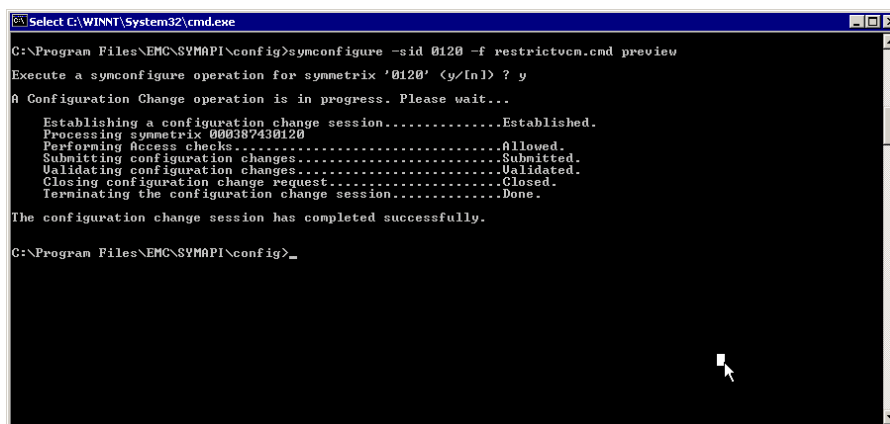
Figure 16 - VCMDB HBA assignments

3) Execute the command file.

You should invoke the `symconfigure` command in stages: the preview argument's first, then prepare, and finally commit if the first two stages succeed. Using the preview and prepare arguments allow you to confirm that the environment will support the requested changes. The preview stage verifies the syntax, most commonly used for debugging. The prepare option performs the preview checks and verifies the appropriateness of the requested configuration changes against the current state of the Symmetrix unit. The commit option performs the previous checking and activates the changes in the Symmetrix unit.

a) Invoke the preview stage to verify syntax and Symmetrix/DMX status:

- i) Run "`symconfigure -sid xxxx -f filename.cmd preview`"



```

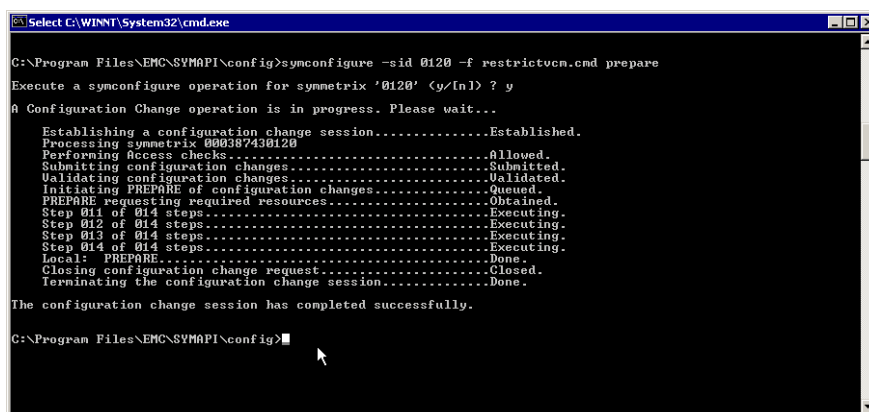
Select C:\WINNT\System32\cmd.exe
C:\Program Files\EMC\SYMAPI\config>symconfigure -sid 0120 -f restrictvcm.cmd preview
Execute a symconfigure operation for symmetrix '0120' <y/[n]> ? y
A Configuration Change operation is in progress. Please wait...
Establishing a configuration change session.....Established.
Processing symmetrix 000387430120.....Allowed.
Performing access checks.....Submitted.
Submitting configuration changes.....Validated.
Validating configuration changes.....Validated.
Closing configuration change request.....Closed.
Terminating the configuration change session.....Done.
The configuration change session has completed successfully.
C:\Program Files\EMC\SYMAPI\config>

```

Figure 17 - "symconfigure" preview stage

b) Invoke the prepare stage to confirm command will execute based on the current Symmetrix status

- i) Run "`symconfigure -sid xxxx -f filename.cmd prepare`"



```

Select C:\WINNT\System32\cmd.exe
C:\Program Files\EMC\SYMAPI\config>symconfigure -sid 0120 -f restrictvcm.cmd prepare
Execute a symconfigure operation for symmetrix '0120' <y/[n]> ? y
A Configuration Change operation is in progress. Please wait...
Establishing a configuration change session.....Established.
Processing symmetrix 000387430120.....Allowed.
Performing access checks.....Submitted.
Submitting configuration changes.....Validated.
Validating configuration changes.....Validated.
Initiating PREPARE of configuration changes.....Queued.
PREPARE requesting required resources.....Obtained.
Step 011 of 014 steps.....Executing.
Step 012 of 014 steps.....Executing.
Step 013 of 014 steps.....Executing.
Step 014 of 014 steps.....Executing.
Local: PREPARE.....Done.
Closing configuration change request.....Closed.
Terminating the configuration change session.....Done.
The configuration change session has completed successfully.
C:\Program Files\EMC\SYMAPI\config>

```

Figure 18 - "symconfigure" prepare stage

c) Invoke the commit stage to activate the configuration change request.

- i) Run “symconfigure –sid xxxx –f filename.cmd commit

```

C:\WINNT\System32\cmd.exe

C:\Program Files\EMC\SYMAPI\config>symconfigure -sid 0120 -f restrictvcn.cmd commit
Execute a symconfigure operation for symmetrix '0120' <y/InI> ? y
A Configuration Change operation is in progress. Please wait...

Establishing a configuration change session.....Established.
Processing symmetrix 000387430120
Performing Access checks.....Allowed.
Submitting configuration changes.....Submitted.
Validating configuration changes.....Validated.
Initiating PREPARE of configuration changes.....Queued.
PREPARE requesting required resources.....Obtained.
Step 003 of 014 steps.....Executing.
Step 011 of 014 steps.....Executing.
Step 012 of 014 steps.....Executing.
Step 013 of 014 steps.....Executing.
Local: PREPARE.....Done.
Initiating COMMIT of configuration changes.....Queued.
COMMIT requesting required resources.....Obtained.
Step 003 of 035 steps.....Executing.
Step 013 of 035 steps.....Executing.
Step 016 of 035 steps.....Executing.
Step 023 of 035 steps.....Executing.
Step 029 of 035 steps.....Executing.
Step 035 of 035 steps.....Executing.
Step 011 of 035 steps.....Executing.
Step 011 of 035 steps.....Executing.
Step 024 of 035 steps.....Executing.
Step 025 of 035 steps.....Executing.
Step 025 of 035 steps.....Executing.
Step 028 of 035 steps.....Executing.
Step 028 of 035 steps.....Executing.
Step 029 of 035 steps.....Executing.
Step 030 of 035 steps.....Executing.
Step 030 of 035 steps.....Executing.
Step 032 of 035 steps.....Executing.
Step 035 of 035 steps.....Executing.
Local: COMMIT.....Done.
Terminating the configuration change session.....Done.

The configuration change session has successfully completed.

C:\Program Files\EMC\SYMAPI\config>_

```

Figure 19 - "symconfigure" commit stage

NOTE: In previous versions of SYMCLI, sometimes a configuration change would not release a lock on the Symmetrix/DMX (SYMCLI bug), prohibiting VCMDB related commands (symmask, symmaskdb, symconfigure) from executing. The following message is displayed:

"The operation failed because another process has an exclusive lock on the local Symmetrix."

In such cases the "symcfg list –lock" command will show the lock# (number) on the Symmetrix/DMX in question. To clear the lock the following command must be invoked:

"symcfg –sid xxxx –force –lockn ## release"

- d) Confirm there are no configuration locks on the Symmetrix/DMX.
i) Run "symcfg list –lock"

```

C:\Program Files\EMC\SYMAPI\config>symcfg list -lock

      S Y M M E T R I X      L O C K S

SymnID      Attachment      Lock      Lock      Lock      Time
              Status        Number    Usage      Held <Sec>
000184502421 Local          Unknown   N/A        N/A        N/A
000387430120 Local          Unknown   N/A        N/A        N/A
000184700743 Remote          Unknown   N/A        N/A        N/A
000185503289 Remote          Unknown   N/A        N/A        N/A
000387430127 Remote          Unknown   N/A        N/A        N/A

C:\Program Files\EMC\SYMAPI\config>

```

Figure 20 - "symcfg list -lock"

- 4) Because this was a Symmetrix/DMX configuration change, an update to the local SYMAPI database is required on all the SAN management hosts attached to the Symmetrix/DMX to reflect the new changes.
 - a) Run "symcfg discover"

```

C:\Program Files\EMC\SYMAPI\config>symcfg discover

This operation may take up to a few minutes. Please be patient...

C:\Program Files\EMC\SYMAPI\config>_

```

Figure 21 - "symcfg discover" - update local SYMAPI database

11.3.1.2. Host Impact Enabling "VCMDB_restricted_access"

Having an already established SAN infrastructure, consideration must be given for current production hosts, for the implementation of "VCMDB_restricted_access".

For example, today the rule-of-thumb for Solaris hosts using "Persistent Binding" is that visibility to LUN0 (vcmdb device) on the Symmetrix/DMX means you have correctly configured SAN zoning for connectivity to the Symmetrix/DMX. As such, this is considered the measuring stick or telltale troubleshooting practice for host connectivity on the SAN to the Symmetrix. Visibility to LUN0 however, does not ensure that one has correctly masked or provisioned the appropriate LUNs on the Symmetrix/DMX.

The impact of enabling "VCMDB_restricted_access" means that LUN0 will no longer be visible to all hosts. This implies that future SAN and Symmetrix/DMX

device provision practices will have to be very detailed oriented, where SAN administrators will be subjected to an “all” or “nothing” success criteria.

GDSE testing of enabling “VCMDB_restricted_access” on Symmetrix 8530 and Symmetrix DMX1000 reported the following responses for legacy-attached SAN hosts:

- Sun Solaris 8 - Hosts with LUN0 configured in “sd.conf reported a configuration error in the “/var/adm/messages” file, with no operational impact. Upon reboot error condition was no longer generated.
- IBM AIX v5.2– hosts reported no error conditions, and no operational impact.
- HP-UX v11.11 – hosts reported no error conditions, there were no implications for contiguous LUNs, and no operational impact.
- Microsoft Win2K Advanced Server – hosts are not usually provisioned to LUN0, and cannot write a signature to the disk. No operational impact.
- VMWARE, ESX Server 2.1 – hosts reported no error conditions, and no operational impact. ESX Server uses Linux RedHat as the underlying OS, as such; expectations are that Linux hosts will respond similarly.

From our test results GDSE certifies that is feasible to safely implement “VCMDB_restricted_access” on current production Symmetrix/DMX.

11.3.1.3. Adding and Removing SAN Management Hosts

Adding and removing additional host HBA's only requires that access is granted or removed from the VCMDB device (0000).

To add additional HBAs invoke the symmask command with the add dev option:

```
“symmask –sid xxxx –wwn 10000000c9xxxxxx –dir ##a –p # add dev 0000”
```

To remove access, invoke the symmask command with the remove dev option:

```
“symmask –sid xxxx –wwn 10000000c9xxxxxx –dir ##a –p # remove dev 0000”
```

Note: Remember to run “symcfg discover” on every SAN Management host post any add or remove of HBAs to the VCMDB device.

11.3.1.4. Disabling “VCMDB_restricted_access”

To remove the Symmetrix/DMX metric "VCMDB_restricted_access" the following steps are necessary:

- 1) Copy the "restrictvcm.cmd" created above to a new file "urestrictvcm.cmd".
- 2) Using your favorite text editor
 - a) edit "urestrictvcm.cmd",
 - b) replace the "enable" option with the "disable" option.
note semi-colon(;) at end of line.
- 3) Save file.

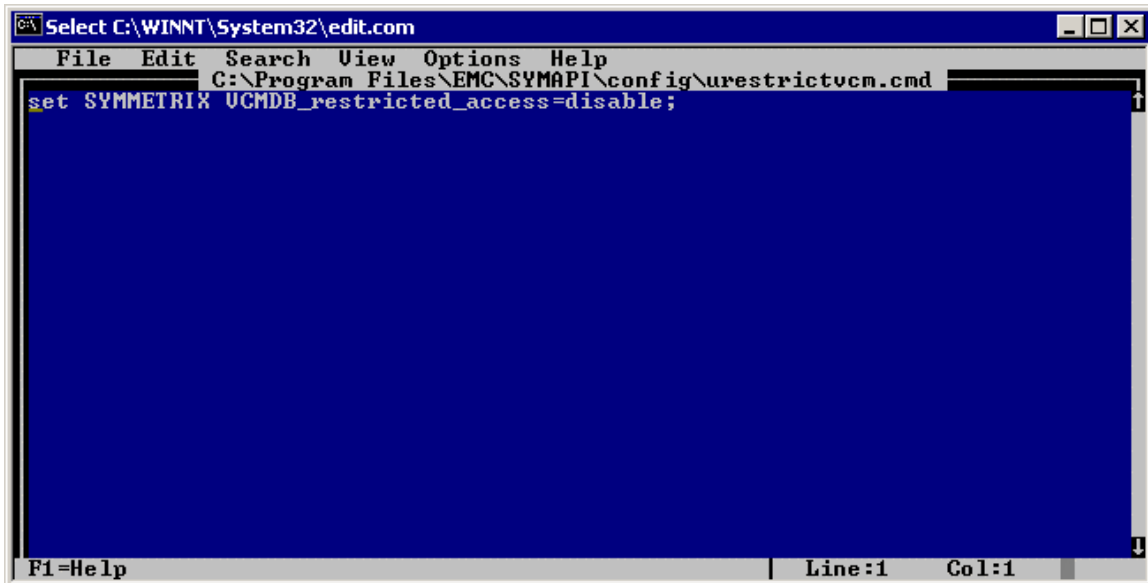


Figure 22 - "VCMDB_restricted_access" disable command file.

- 4) Run the "symconfigure" command in all its stages.
- 5) Run "symcfg discover" on every SAN Management host to update the local SYMAPI database.

In addition, as mentioned earlier, if access from all SAN Management host is lost, the local EMC CE or EMC phone support analyst can remove the option from the Symmetrix/DMX service processor.

11.3.2. SYMACL – Symmetrix/DMX Host Access Control Management

Today, anyone with access to Symmetrix-based management software can execute any function on any Symmetrix device. EMC Solutions Enabler (SYMCLI) supports the "symacl" command component that allows you to set up and maintain an access-controlled environment over the Symmetrix/DMX resources (device pools).

The symacl database uses the following access control mechanisms to govern access to the Symmetrix/DMX device pools:

- *Access control groups* - Unique *access IDs* and *names* are assigned (together) to hosts and users and then sorted into *access control groups* according to similar needs (determined by an Administrator). Access groups are allowed to act on device pools based on *rights (access types)* granted by the Administrator.

The unique host ID for open systems can be viewed by running “symacl – unique”

- *Device pools* - Access rights (types), such as BCV, SRDF, ADMIN, give permission to a host or user to perform certain Solutions Enabler functionality on a specified device pool. Device pools are sometimes referred to as access pools or accpool.
- *Access control entries (ACES)*- Once the group and device pool mechanisms are established, the *access control entries (ACEs)* are created, which grant access rights to these pools. The ACEs of the various access groups (along with groups and pools) are managed and stored in the access control database.
- *Access control list (ACL)* - is a group of ACEs that are associated with the same “accgroup”. For example, the ACEs that are associated to a control group comprise an ACL in the database.

The following table illustrates a Symmetrix/DMX that is managing the access rights of various types of host connections to the Symmetrix devices. Each Symmetrix has its own access control database, which are separately managed by “symacl”.

Groups		Device Pools		ACE/ACLs		
Name	AccessID (hostname)	Name	Devices	accgroup	rights	dev/accpool
AdminGrp	SunHost1	ProdDevs	002 - 011 01C - 01F	UnknwGrp ACE	ALL	ALL_DEVS
ProdB	WinHost	PoolA	012 - 019 022 - 02A	AdminGrp ACE	BASE	ALL_DEVS
HR	WinHR1	PoolHR	081 - 0AA	AdminGrp ACE	ADMIN	ALL_DEVS
Sales	WinSale2	SalePool	03A - 03F	ProdB ACE	BASE	PRODdevs
GroupA	UXNodeB			ProdB ACE	RDF	PRODdevs
UnknwGrp	Default			HR ACE	BASE	PoolHR
				HR ACE	BCV	PoolHR
				Sales ACE	BASE	Salepool
				Sales ACE	SDR	Salepool
				GroupA ACE	ALL	PoolA

Table 1 - Sample "symacl" database entries

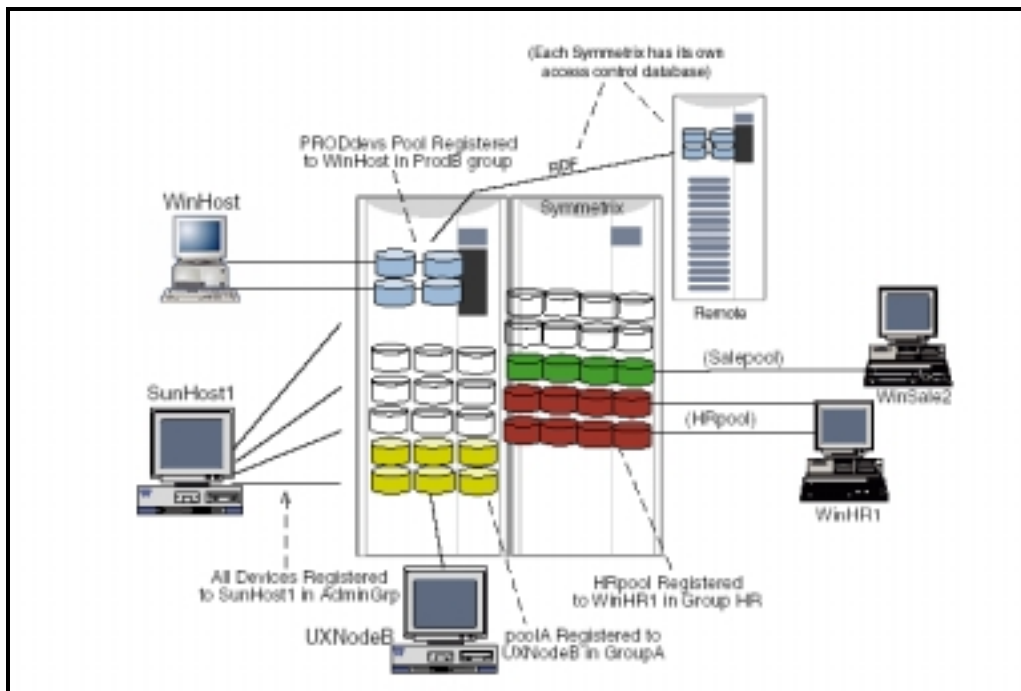


Figure 23 - Sample Symmetrix/DMX "symacl" configuration

Like "symconfigure", "sycacl" uses a command file to create or change the access control information in the database. The following are the various types of rights creation and changes possible in the command file:

- Create new access groups
- Add and remove access IDs to access groups
- Move an access ID from one group to another
- Create new device pools
- Add and remove devices to device pools
- Delete device pools and access groups
- Add ACEs to grant access
- Remove ACEs to deny access

11.3.2.1. SYMACL Symmetrix/DMX Setup

Initial setup of "symacl" requires the EMC CE to configure a SAN Management host for minimal access control parameters to enable you to begin administrative actions. From the SAN Management host the following is required:

- Symmetrix Serial number: 000387430120
- Host ID ("symacl -unique"): 2F5802AF-524389CF-993D757A
- Host Name (up to 8 characters): *sangs7*
- User Name (up to 8 characters): *gdseacis*
- User ID: 0120 (*Note this is also the SYMACL_ACCESS_PIN*).

The Symmetrix serial number and symacl Host Id are specific to the Symmetrix/DMX and SAN Management host respectively. All other variables are user defined and need only follow restrictions for character length.

These variables can be gotten using the following symcli commands:

- Symmetrix/DMX S/N
 - o `symcfg list`

```

C:\WINNT\System32\cmd.exe
C:\>symacl -unique
The unique id for this host is: 2F5A05A6-54408EC9-99367578
C:\>symcfg list

      S Y M M E T R I X

SymnID      Attachment  Model      Mode  Cache  Num Phys  Num Symm
              Version      Size <MB>  Devices Devices
000184502421 Local      8530      5568    16384      3      411
000387430120 Local     1000S-M2  5670    16384      8     1075
000184700743 Remote     8730      5568    32768      0      411
000185503289 Remote     8530      5568    16384      0      791
000387430127 Remote    DMX1000S  5670    24576      0      563
  
```

Figure 24 – Host and Symmetrix/DMX variables required for initial setup of symacl

- Host ID (The symacl -unique option returns the encrypted access ID in the following segmented, 24-digit numeric form:

xxxxxxx-yyyyyyy-zzzzzzzz
o symacl -unique

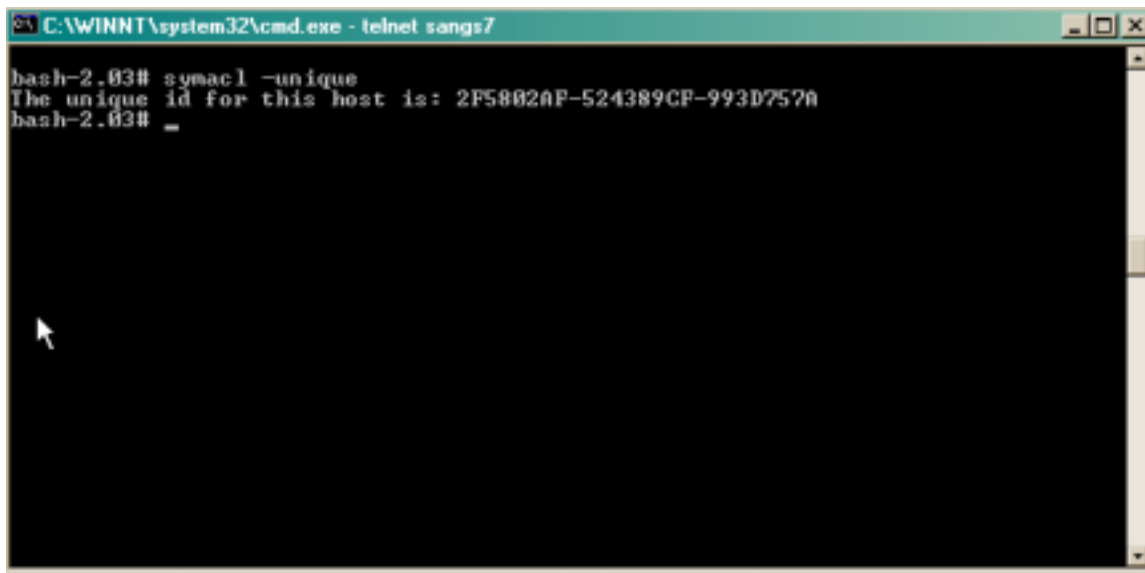


Figure 25 - "SYMACL -unique" HOST ID

11.3.2.2. Default Configuration

Typically following initial setup of "symacl" on a Symmetrix/DMX the database contains the following default ACLs:

Groups		Pools		ACE/ACLs		
Name	Access/ID (hostname)	Name	Devices	accgroup	rights	dev/accpool
AdminGrp	SANADx	!INPOOLS	001 - FFF	AdminGrp ACE	ALL ADMIN	ALL_DEVS
UnknwGrp	Default			UnknwGrp ACE	ALL	!INPOOLS
				UnknwGrp ACE	BASE	ALL_DEVS

Table 2 - Default "symacl" ACLs setup

As shown in the above table for an initial setup, access group AdminGrp has access to all devices (ALL_DEVS) and this group was granted both ADMIN and ALL rights. In addition, a group called UnknwGrp was established for unknown users, making all devices in the Symmetrix accessible to this unknown group. By default, this gives all unknown hosts BASE rights to all devices (ALL_DEVS) until such time it becomes clear as to what restrictions should be established. The initial UnknwGrp setup also grants ALL rights to (!INPOOLS), where all devices not already assigned to an "accpool" are pooled by default.

11.3.2.3. Access Group Management

To set up an access control group, you need to create a group and then add the various access IDs of the hosts and users as members of that group.

Creating Access Groups

To set up an access control group, you need to create a group and then add the various access IDs of the hosts and users as members of that group. Group names are limited to 8 characters or less.

- 1) From the SAN Management host (SANADx): create a command file (addnewgroups.cmd),
 - a) Create file "addnewgroups.cmd"
 - b) enter:
create accgroup storint;
create accgroup storeng;
 - i) save file.
- (NOTE: semi-colon (;) at end of each line)

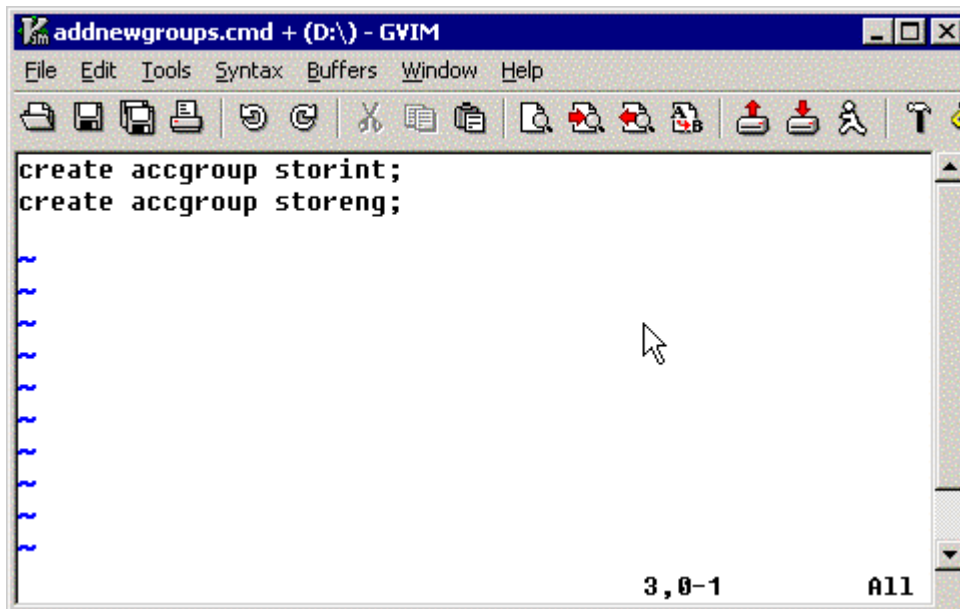


Figure 26 - symacl creating accgroup command file syntax

- 2) Commit the file (addnewgroups.cmd) that executes the creation of the groups, enter:
 - a) "symacl -sid xxxx commit -file addnewgroups.cmd"
 - b) At this point, you may be prompted for your 4 - 12 character access PIN (if environment variable SYMCLI_ACCESS_PIN is not already set to this PIN value).

Adding Host Access Ids to a Group

To add a host access ID to an access group, use the following syntax in the command file:

add host accid *Id* name *IdName* to accgroup *GroupName*;

- 1) Edit (addnewgroups.cmd), add the following line:
 - a) "add host accid 2F5A05A6-54408EC9-99367578 name emcsrv07 to accgroup AdminGrp;"

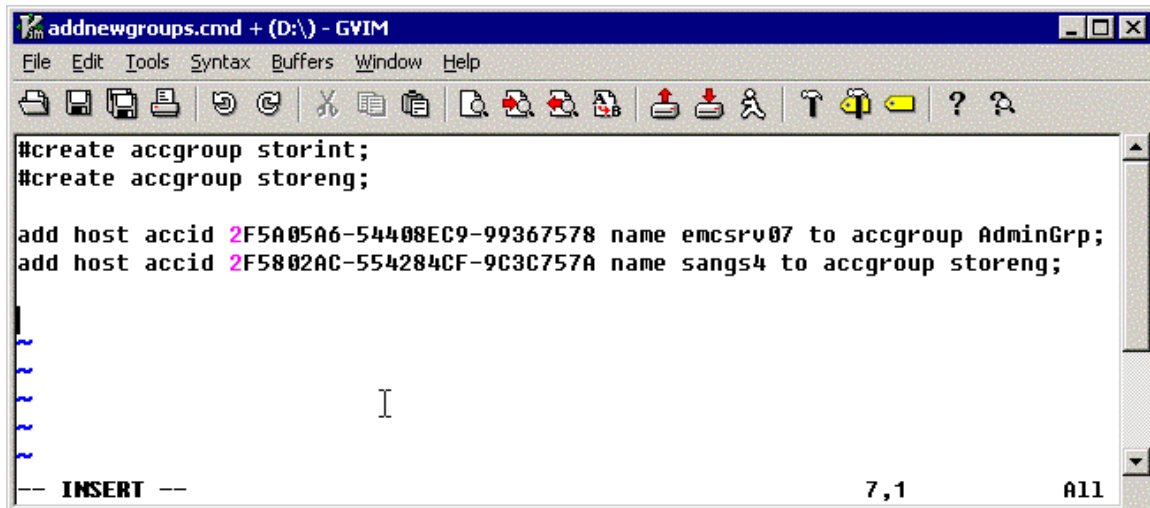


Figure 27 - symacl adding host Access ID command file syntax

11.3.2.3.1. Add User Access Ids to a Group

User Access IDs are 4 - 12 character passwords or PINs defined by the users. When a user attempts a commit, prepare, or release operation, symacl prompts the user for a PIN. To add a user access ID to an access group, use the following syntax in the command file:

add user accid *Id* name *IdName* to accgroup *GroupName*;

- 1) Edit (addnewgroups.cmd), add the following line:
 - a) "add user accid 0120 name gdseac1s to accgroup engineering;"

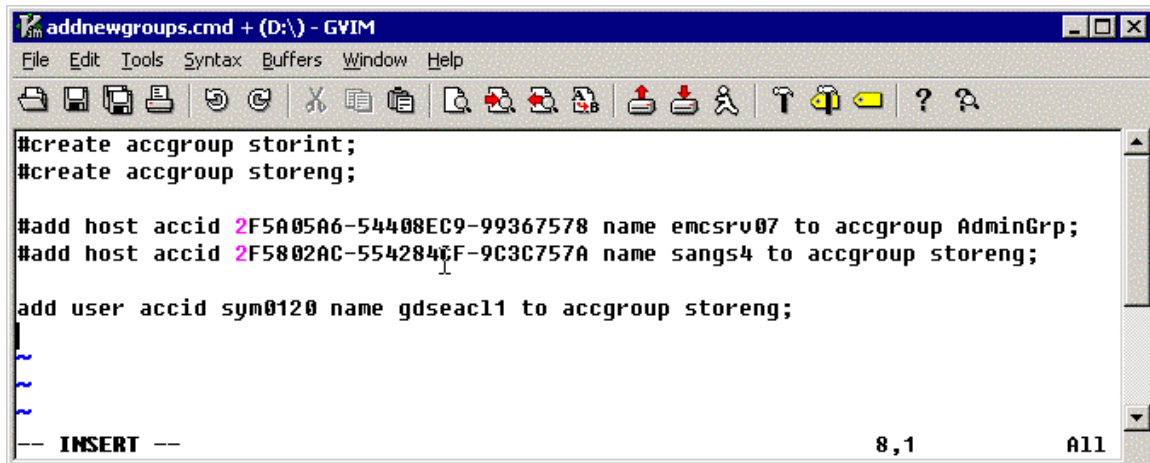


Figure 28 - symacl adding User Access ID command file syntax

11.3.2.3.2. Access Group Maintenance

Once access groups are established, you can remove access IDs or ACEs from a group, move IDs from one group to another, or delete an entire group.

- Remove a host accid from a Group - To remove an access ID from an access group, use the following syntax in the command file:
 - o remove accid name *IdName* from accgroup *GroupName*;
- Move an Access ID to Another Group - To move an access ID from one access group to another, use the following syntax in the command file:
 - o move accid name *IdName* to accgroup *GroupName*;
- Remove all ACEs from a Group - To remove all ACEs from an access group, use the following syntax in the command file:
 - o remove aces from accgroup *GroupName*;
- Delete a Group - To delete an access group from the database, use the following syntax in the command file:
 - o delete accgroup *GroupName* [remove_aces=true];

Note: All ACEs must be removed before you can delete a group, or you can use the “remove_aces=true” option in the command to remove all ACEs at the same time.

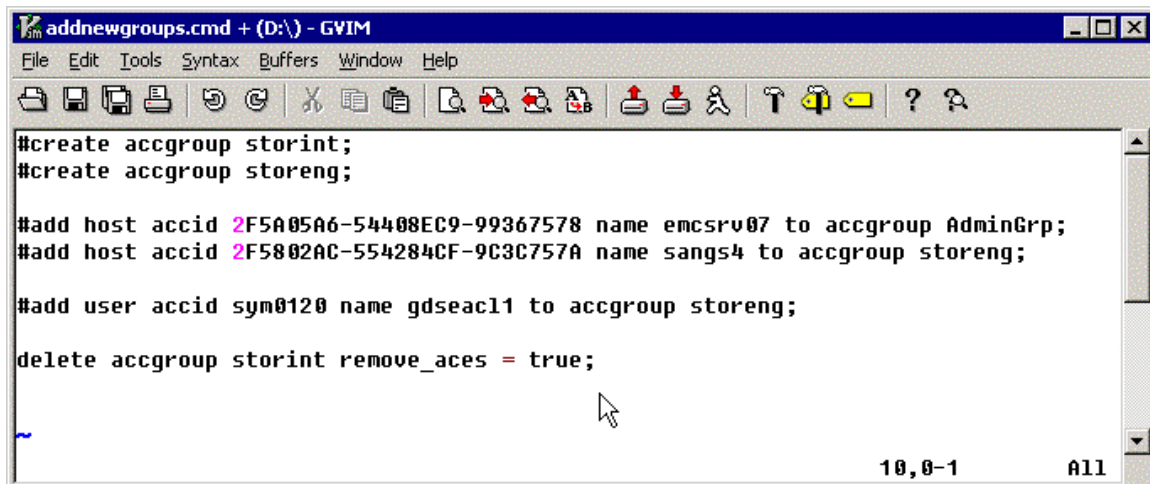


Figure 29 - symacl Delete Access Group command file syntax

11.3.2.4. Device Pool Management

When the various Symmetrix devices used by a host application must function as non-shareable resources, the target devices must be identified and assigned into a device pool for protection. Once a device pool is created, the pool can be a target to create access control entries (ACEs). More than one access group can access a pool with different rights.

Create a Device Pool

To create a Device Pool you must first create the pool and later add the specific Symmetrix/DMX devices that will be controlled by Access Groups.

From the SAN Management host (SANADx):

- 1) Using your favorite editor, create a command file and add the appropriate Pool name:
 - a) Edit addnewpool.cmd, add the following command:
 - i) "create accpool engBCV;"

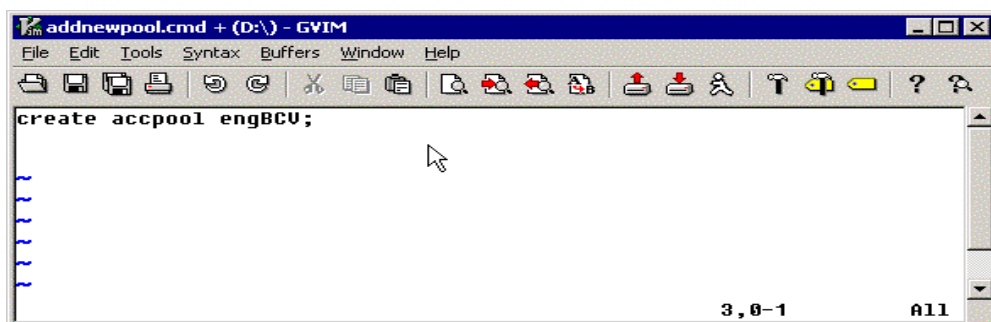


Figure 30 - symacl create accpool command file syntax

Add Devices to a Pool

- 1) Edit the command file `addnewpool.cmd`, use the following syntax ;
 - a) add dev *StartDevName[:EndDevName]* to accpool *PoolName*;
 - i) “add dev 0001:0200 to accpool engBCV;”

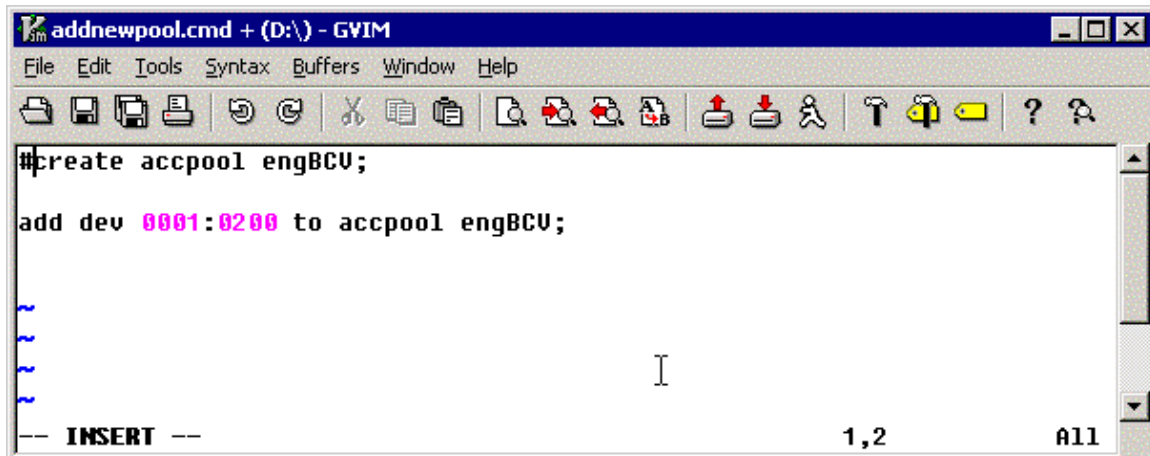


Figure 31 - symacl add dev to accpool command file syntax

Device Pool Maintenance

You can edit and manage the existing device pool information in the access control database.

- Remove Devices from a Pool - To remove specific Symmetrix devices from a pool, use the following syntax in the command file:
 - o remove dev *StartDevName[:EndDevName]* from accpool *PoolName*;
- Delete a Device Pool - To delete a device pool and remove all ACEs, use the following syntax in the command file:
 - o delete accpool *PoolName* [remove_aces=true];

Note: All ACEs must be removed before you can delete a pool, or you can use the “remove_aces=true” option in the command to remove all ACEs at the same time.

11.3.2.5. ACE/ACLs Management

Once you have created groups and device pools, you can now create access control entries (ACEs) that grant access rights to the groups and pools. A group can have multiple access rights and pools, which requires an ACE for each.

The rights (*AccessType*) granted to a group for a specified device pool uses the following command file syntax:

"grant access=<AccessType,,> to accgroup GroupName for <accpool PoolName> | <ALL|NON-POOLED devs>,"

The *AccessType* parameter specifies the rights to the SYMCLI or SYMAPI features or functionality that is to be granted to selected devices.

The following table describes the possible rights (*AccessType*) available to symacl-managed hosts on the Symmetrix DMX:

Rights (AccessType)	Rights Description	Commands Affected
ADMIN ^a	Grants administrator privilege to grant/deny access control entries to hosts and users.	symacl <prepare, commit, release, list, show>
ADMINRD ^a	Grants read access only to all access control information.	symacl <list, show>
ALL ^c	All possible access types granted except ADMIN and ADMINRD. Must be directed to ALL devices.	All
BASE ^a	Allows the discovery of devices and to obtain states and statistics from the Symmetrix array (directors and devices). Must be directed to ALL devices.	Base component commands
BASECTRL	Allows base control operations on devices and device groups.	symld <controls>
BCV	Allows TimeFinder (BCV) control and status operations.	symmir <controls>
BDF	Allows FasTrax functionality.	Not implemented
CACHCTRL	Allows Cache control operations concerning LRU partition management.	symqos <set LRU >
CFGDEV	Allows powerful configuration control operations that manage various types of configuration changes on devices in the Symmetrix.	symconfigure
CFGSYM ^c	Allows access to set Symmetrix attributes, set port flags, and swap RA groups with symconfigure. Must be directed to ALL devices.	symconfigure
CHECKSUM	Allows Symmetrix device Oracle checksum operations.	symchksum <controls>
CREATEDV ^c	Allows the creation of Symmetrix devices (part of symconfigure). Must be directed to ALL devices.	symconfigure

DIRCTRL ^c	Allows you to take directors and their ports offline and online. Must be directed to ALL devices.	symcfg <online/offline>
ECC ^{ab}	Allows the ECC symmetrix agent to run on the requested host.	Not applicable
ERASE	EMC Symmetrix Secure Erase allows the user to permanently and securely erase Symmetrix devices.	symerase
OPTMZR	Allows user configurable attributes that may affect the Optimizer behavior.	symoptmz <controls>
POWRPATH ^{bc}	Access to PowerPath-directed devices in an RDF consistency group. Must be directed to ALL devices.	Not applicable
QOS	Allows the execution of Quality of Service (QOS) performance control operations. Excludes LRU cache control functionality.	symqos <set pace>
RDF	Allows SRDF control and set operations.	symrdf <control
SDDF	Allows the DeltaMark™ (Change Tracker) functionality that monitors track changes.	symchg
SDR	Allows mapping/unmapping of devices to directors/ports for the Symmetrix Disk Reallocation (SDR) feature.	symconfigure
SNAP	TimeFinder/Snapshot allows the creation and management of virtual copy sessions between a source device and multiple virtual (VDEV) target devices.	symsnap
VLOGIX ^{bc}	Enables access to Device Masking or Volume Logix devices.	symmask, symmaskdb
a. Note that this access type can only be specified for all the devices in a Symmetrix and cannot be specified for device pools.		
b. See the appropriate product documentation for use of these access types.		

c. These access types must be granted to either ALL devices or all NON-POOLED devices in a Symmetrix.

To effectively manage access controls in the Citigroup SOE SAN infrastructure the following symacl rights (AccessTypes) must be adhered to:

Green Rights – SAN Management Hosts (SANADx) only.

Yellow Rights – SAN Application Hosts requiring BCV and or RDF functionality.

Red Rights – These rights are inherent in the ADMIN rights and should not be required of any Application hosts, unless business justification implies otherwise.

Grant Rights (AccessType) to an Access Group

To grant “ADMIN” rights to all devices “ALL DEVS” for group “storeng” the following sequence must be completed:

- 1) From the SAN Management Host (SANADx), create a command file:
 - a) Edit “addnewrights.cmd”
 - b) Enter the following command syntax:
 - i) Grant access=BASE to accgroup storing for accpool ALL DEVS;
 - ii) grant access=ADMIN to accgroup storeng for accpool ALL DEVS;

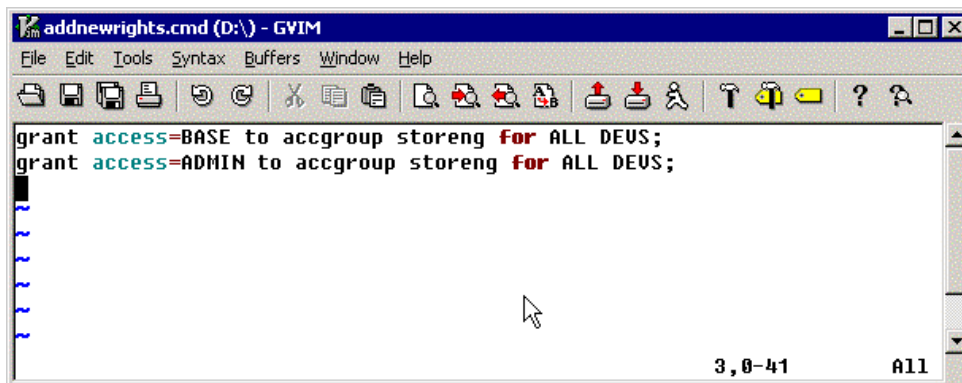


Figure 32 - granting symacl rights command file syntax

- c) commit command file:
 - i) symacl -sid xxxx -f addnewrights.cmd commit

NOTE: Before you can grant a group the rights to any value-added non-base feature, you must first grant the group BASE rights to all devices.

Remove Rights (Access Type) from an Access Group

To remove rights for an access group, use the following command in the command file:

```
remove access=<AccessType,,,> from accgroup GroupName for <accpool PoolName> | <ALL|NON-POOLED devs>;
```

NOTE: At some point, you must commit the command file to execute the changes with the entries. In addition, you should execute the “symcfg configure” command after every configuration change in order to update the SYMAPI database.

11.3.2.6. Access Control Information

You can check the current Symmetrix/DMX access control database to view the various groups, pools, and also the ACLs. Only if you have ADMIN or ADMINRD rights, can you view all access objects in the access control database.

Listing Access Control information

Using the list argument in the following command, you can list information about groups, pools, and ACLs with the following syntax:

- `symacl [-sid SymmID|ALL] list -accgroup | -accpool | -acl | -v`

Showing Access Control Information

Using the show actions when you don't have administrative rights, you only see access objects that are associated with the access group to which your host belongs. To show detail information about a specified group or pool, use the following syntax:

- `symacl -sid SymmID|ALL show accgroup GroupName | show accpool PoolName`

11.3.2.7. SYMACL Backup and Restore

EMC has recently included the ability to backup and restore the symacl database. As a best practice, GDSE recommends, a backup copy of the symacl database be created before and after any symacl configurations are made

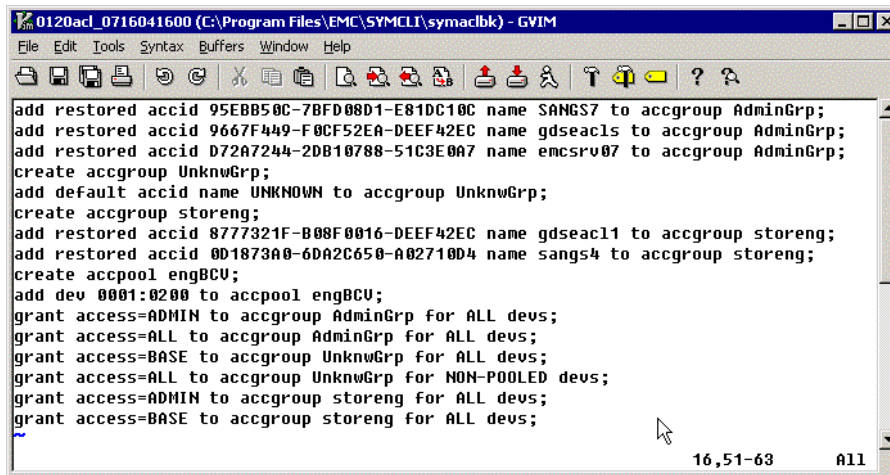
11.3.2.7.1. Symacl Backup

The backup operation saves the contents of the access control database in the file specified by the file option. The file must not previously exist. The backup file created is a text command file compatible for use with the symacl utility.

To create a backup of the symacl database, use the following command:

`symacl -sid SymmID backup -file CommandFile`

Note: The backup file contains encrypted versions of the unique IDs, therefore if you compare the values in the backup file to the original file used to create the database, they will be different.



The screenshot shows a GVIM editor window titled "0120acl_0716041600 (C:\Program Files\EMC\SYMCLI\symaclbk) - GVIM". The window contains a list of commands for managing access control groups and pools. The commands are as follows:

```
add restored accid 95EBB50C-78FD08D1-E81DC10C name SANGS7 to accgroup AdminGrp;  
add restored accid 9667F449-F0CF52EA-DEEF42EC name gdseac1s to accgroup AdminGrp;  
add restored accid 072A7244-2DB10788-51C3E0A7 name emcsrv07 to accgroup AdminGrp;  
create accgroup UnknwGrp;  
add default accid name UNKNOWN to accgroup UnknwGrp;  
create accgroup storeng;  
add restored accid 8777321F-B08F0016-DEEF42EC name gdseac11 to accgroup storeng;  
add restored accid 001873A0-6DA2C650-A02710D4 name sangs4 to accgroup storeng;  
create accpool engBCV;  
add dev 0001:0200 to accpool engBCV;  
grant access=ADMIN to accgroup AdminGrp for ALL devs;  
grant access=ALL to accgroup AdminGrp for ALL devs;  
grant access=BASE to accgroup UnknwGrp for ALL devs;  
grant access=ALL to accgroup UnknwGrp for NON-POOLED devs;  
grant access=ADMIN to accgroup storeng for ALL devs;  
grant access=BASE to accgroup storeng for ALL devs;
```

The status bar at the bottom right of the window shows "16,51-63" and "All".

Figure 33 - symacl backup file command file syntax

11.3.2.7.2. Symacl Restore

The restore operation replaces the contents of the access control database with the contents of the file specified by the file option. It eliminates whatever currently exists in the Symmetrix/DMX configuration database and replaces it with the contents of the backup file.

To restore a backup using symacl you use the `-restore` option as shown below:
`symacl -sid SymmID commit [-v|-noecho] -restore -file CommandFile`

```

C:\WINNT\System32\cmd.exe
C:\Program Files\EMC\SYMCLI\syclbk>symacl -sid 0120 commit -restore -file 0120acl_0716041600
Enter Access PIN:
Command file: <0120acl_0716041600>
PREVIEW.....Started.
PREVIEW.....Done.
PREPARE.....Started.
  Adding Restored access id SANGS7 to group AdminGrp.....Done.
  Adding Restored access id gdseac1s to group AdminGrp.....Done.
  Adding Restored access id emcsrv07 to group AdminGrp.....Done.
  Creating group UnknwGrp.....Done.
  Adding the DEFAULT access id UNKNOWN to group UnknwGrp.....Done.
  Creating group storeng.....Done.
  Adding Restored access id gdseac1l to group storeng.....Done.
  Adding Restored access id sangs4 to group storeng.....Done.
  Creating pool engBCV.....Done.
  Adding 512 devs, dev 0001 through 0200 to pool engBCV.....Done.
  Granting access ADMIN to group AdminGrp for ALL devs.....Done.
  Granting access ALL to group AdminGrp for ALL devs.....Done.
  Granting access BASE to group UnknwGrp for ALL devs.....Done.
  Granting access ALL to group UnknwGrp for NON-POOLED devs.....Done.
  Granting access ADMIN to group storeng for ALL devs.....Done.
  Granting access BASE to group storeng for ALL devs.....Done.
PREPARE.....Done.
Starting COMMIT.....Done.
C:\Program Files\EMC\SYMCLI\syclbk>
C:\Program Files\EMC\SYMCLI\syclbk>symacl -sid 0120 commit -restore -file 0120acl_0716041600_

```

Figure 34 - symacl database -restore command syntax

11.3.3. Strategy for Hosts requiring BCV/Symmir Controls

To set up an access-controlled environment for BCV/Symmir operations, you need set up both the standard and BCV devices as follows:

- 1) Define the working device pool to contain both the STD and BCV Symmetrix device names.
- 2) For the group name, grant BASE rights to access all devices.
- 3) For the group name, grant BCV rights to the device pool holding the pairs.

11.3.4. Strategy for Hosts requiring SRDF Controls

To set up an access-controlled environment for SRDF operations, you need set up both the local and remote Symmetrix/DMX. Because both Symmetrix arrays have their own access-controlled database, you must:

- 1) From the SAN Management Host (SANADx), create an access control group for the local Symmetrix/DMX. Then with a local or remote SANADx host, define the same access control group name for the remote Symmetrix.
- 2) From the SANADx host, create a device pool defined with the R1 Symmetrix/DMX device names. Then with the local or remote SANADx host, define a device pool on the remote Symmetrix/DMX with the R2 Symmetrix/DMX device names.
- 3) Grant BASE rights for the local group to access all devices. On the remote SANADx host, grant BASE rights for the group (created in step 1) to access all devices.
- 4) Grant RDF rights for the local group to access the R1 device pool. From the remote 0SANADx host, grant RDF rights for the group to access the R2 device pool.

11.3.5. GDSE Recommended Access Control Strategy

The policy for complete control of the Symmetrix/DMX, is to only register access to certain devices on an as-needed basis. To accomplish this, the UNKNOWN user ACEs and userID are removed from the UnknwGrp. Therefore, the Symmetrix/DMX must know the application host/node, and only specific users/hosts in defined groups with limited or unlimited rights have access to the devices defined in their working pools.

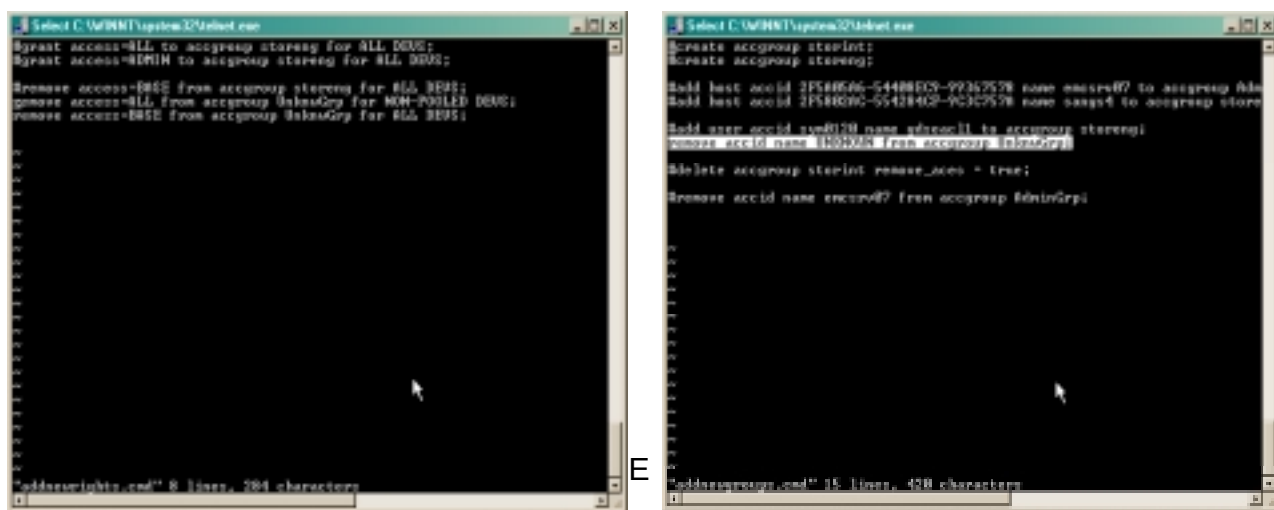


Figure 34 - UnknwGrp - remove ACEs and UserID

11.4. Confidentiality and integrity

In order to maintain the confidentiality of business information stored on the array, the following processes should be implemented⁶:

- o Before a disk is returned to the vendor, all information on the disk must be erased
- o Before a logical disk (“LUN”) is re-assigned, all information on the LUN must be erased

11.5. Incident detection and response

The array maintains a log of system administration activities. This log can be obtained by using the “symaudit” CLI command. A sample output from this command is shown in appendix E.

This log should be archived and reviewed periodically.

11.6. Administration

This component does not initiate, program, process, or authorize business transactions. This product does not internally support segregation of system and security administration or maker/checker functions. There are no default capabilities that can be disabled or protected.

⁶ Detailed procedures are expected to be available by end of 2004

12. Solutions Enabler

12.1. Introduction

The Solutions Enabler application from EMC is a collection of command line tools that are used to manage the Symmetrix storage array. These command line tools are installed on a SOE server connected to the SAN. The tools communicate with the 'gatekeeper' device on the array via the fibre channel network.

Solutions Enabler can be deployed in a client-server topology. In this configuration, the "SYMAPI" server allows clients to issue commands to manage the array over a TCP/IP network.

12.2. Identification and Authentication

The tools that make up the Solutions Enabler product do not authenticate or authorize users. As a compensating control, the tools should only be accessible after authentication against a SOE server. This is enabled by the topology illustrated in figure 31.

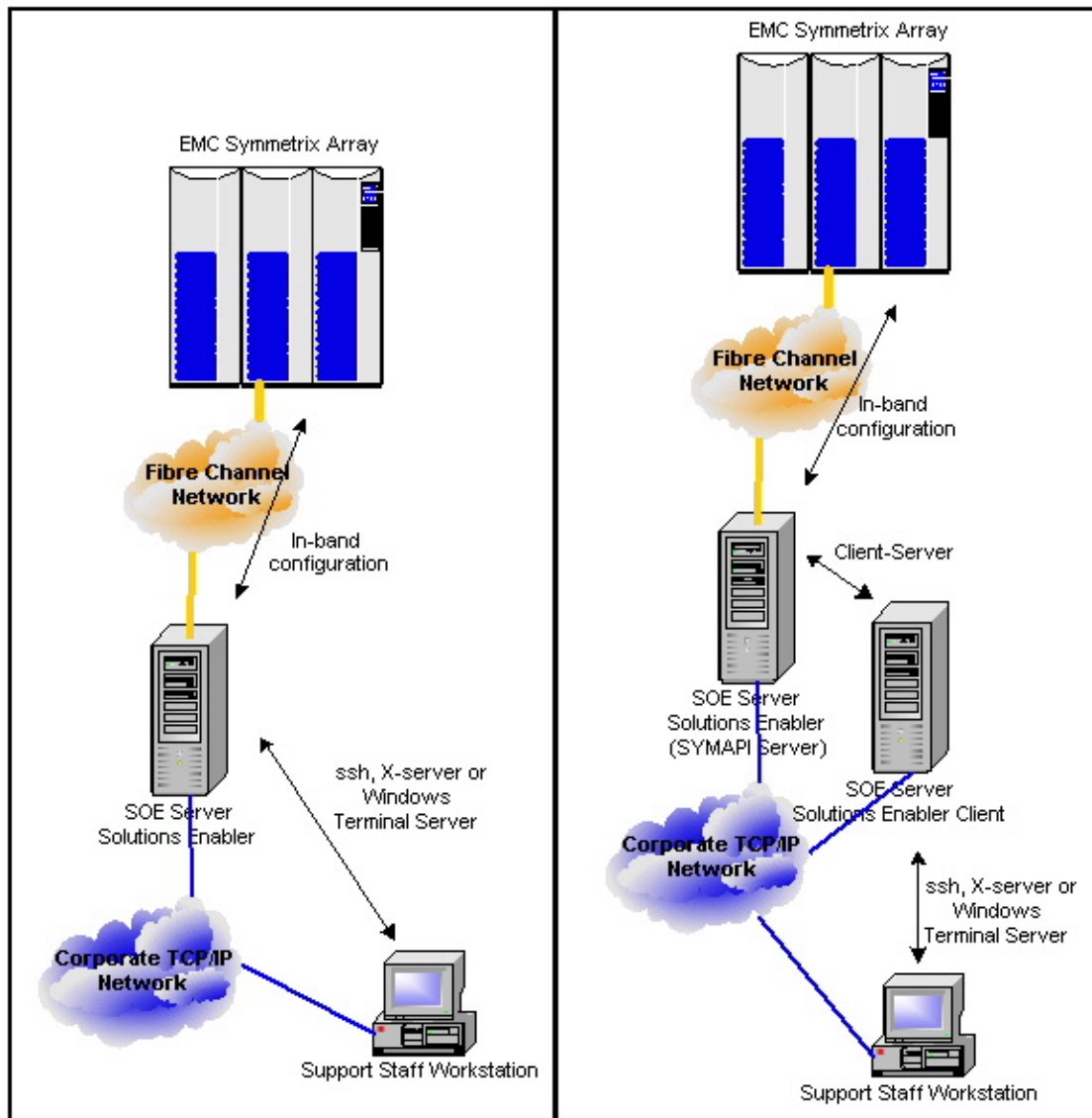


Figure 35 Secure Topology for Solutions Enabler

12.3. Authorization and access control

Because Solutions Enabler does not identify users, it does not have any access control capabilities. Access to the tool is restricted by hosting the application on a SOE server that has been authorized access to the Symmetrix with SYMACL. Logon to this SOE server should be limited to staff authorized by Storage Management.

If the client-server model is used, the **nethost** file should contain entries for each host that can connect as a client. Wildcards, that would permit all hosts to connect, should not be used.

12.4. Confidentiality and Integrity

The component does not process or store business information. There are no configurable elements.

12.5. Incident detection and response

This component does not generate any logs. System administration actions are recorded on the Symmetrix array instead. Please see the Symmetrix section for details.

12.6. Administration

This component does not initiate, program, process, or authorize business transactions. This component does not internally support segregation of system and security administration or maker/checker functions. There are no default capabilities that can be disabled or protected.

13. Brocade Switch

13.1. Introduction

The Brocade fibre channel switch provides highly available and scalable connectivity between hosts and array ports. The Brocade switch can be accessed with the following protocols:

Access Protocol	Network Protocol	Remarks
CONSOLE	None	Serial console. Used for managing the switch
TELNET	TCP/IP	Used for managing the switch
HTTP	TCP/IP	Called "webtools". Used for managing the switch
SNMP	TCP/IP	Used for managing the switch
N_PORT	FC	Used by hosts to connect to the FC network
E_PORT	FC	Used for interconnecting switches
PROPRIETARY (Brocade API)	TCP/IP	Used for managing the switch

13.2. Identification and authentication

The Brocade switch does not identify users. It uses two built-in IDs that are assigned built-in privileges. To compensate, the Brocade switch should only be accessible after authentication to a SOE server. This is accomplished by connecting the Brocade switch on a private TCP/IP network, and using a dual homed SOE server for managing the switch.

13.3. Authorization and access control

The switch has the capability of controlling access to array ports based on the host identity, which is the WWN. Switch ports can be "zoned" to specific array ports. Several types of zoning are available, some more secure than others. Today, the company standard is to use WWN based zoning. Unfortunately, this type of zoning is designed to work in co-operation with the host bus adaptor driver. If the HBA driver so chooses, it can ignore the zoning configuration and communicate to unauthorized array ports, possibly gaining access to unauthorized disk resources.

The secure alternative to WWN zoning is "port zoning". Although this technology is available on the installed base, it is not recommended since it has a large, negative impact on the storage provisioning process.

Because of the above weakness in the WWN zoning, it cannot be considered as a reliable control⁷ for the purpose of this guide.

In the future, fibre channel switches will be able to enforce WWN zoning by actively inspecting and blocking fibre channel frames that do not meet the zoning criteria. Combined with a DH-CHAP based authentication, this technology is expected to provide a reliable access control mechanism at the switch level.

The lack of access control at the switch level is adequately compensated by the access controls on the storage array. These controls are discussed later in this document.

For the management interfaces, the Brocade switch has role based access control. Two roles are provided – administrator and user.

The SOE server used for managing the switch should be configured to limit logon to staff authorized by Storage Management.

Further, Storage Management should create level 3 procedures to ensure that passwords for the built-in IDs on the switch are six or more alphanumeric characters, and that these passwords are changed periodically.

13.4. Confidentiality and Integrity

The component does not process⁸ or store business information. There are no configurable elements.

13.5. Incident detection and response

The Brocade switch is capable of recording events to an external system via SNMP Traps and/or syslog, as illustrated in Appendix F. However, because the switch does not identify users, these logs carry very little meaning from an Information Security perspective. Archival and review of these logs is therefore not considered necessary.

13.6. Administration

This component does not initiate, program, process, or authorize business transactions. This product does not internally support segregation of system and security administration or maker/checker functions.

The following default capabilities should be disabled or protected:

⁷ WWN zoning should still be used as it resolves issues related to availability and serviceability of the SAN and provides additional, albeit insufficient controls over no zoning.

⁸ Even though business information passes through the switch, there is no interface for access

- Change the default passwords for the administrator and user built-in IDs at the time of installation
- When the SNMP agent on the switch is not being used, it should be disabled. This can be done by clearing the community strings in the “Community and trap recipient configuration” as shown in figure 32.

Switch Admin for fabric2sw1 - Microsoft Internet Explorer

SwitchName: fabric2sw1 DomainId: 21 WWN: 10:00:00:60:69:50:0a:11 Tue Apr 13 2004, 5:39 PM

Trunk Information QuickLoop Remote Switch Extended Fabric

Report Port Setting User Admin Configure Routing

Switch Settings Network Config Firm Upgd **SNMP** Lic Admin

SNMP Information

Name: GDSE Description: a_fabric2sw1

Location: 388 Greenwich 12 Floor Trap Level: 0

☐ Enable Authentication Trap

Community And Trap Recipient Configuration

Community String	Recipient	Access Control List
0.0.0.0	0.0.0.0	READ ONLY
0.0.0.0	0.0.0.0	READ ONLY
0.0.0.0	0.0.0.0	READ ONLY
0.0.0.0	0.0.0.0	READ WRITE

Access Control List Configuration Enter a valid IP address

Access Host	Access Control List
0.0.0.0	1 - READWRITE
0.0.0.0	1 - READWRITE
0.0.0.0	1 - READWRITE
0.0.0.0	1 - READWRITE

OK Apply Close Reset

Switch Commit Messages

SNMP Panel

Figure 36 Disabling the SNMP agent on the Brocade switch

- If the SNMP agent is to be used, a community string that is six or more alphabetic and numeric characters should be used. Please see figure 33.

Switch Admin for fabric2sw1 - Microsoft Internet Explorer

SwitchName: fabric2sw1 DomainId: 21 WWN: 10:00:00:60:69:50:0a:11 Tue Apr 13 2004, 5:41 PM

Trunk Information QuickLoop Remote Switch Extended Fabric

Report Port Setting User Admin Configure Routing

Switch Settings Network Config Firm Upgd **SNMP** Lic Admin

SNMP Information

Name: GDSE Description: a_fabric2sw1

Location: 388 Greenwich 12 Floor Trap Level: 0

☒ Enable Authentication Trap

Community And Trap Recipient Configuration

Community String	Recipient	Access Control List
zwx2234	154.65.23.4	READ ONLY
	0.0.0.0	READ ONLY
	0.0.0.0	READ ONLY
	0.0.0.0	READWRITE

Access Control List Configuration

Access Host	Access Control List
0.0.0.0	1 - READWRITE
0.0.0.0	1 - READWRITE
0.0.0.0	1 - READWRITE
0.0.0.0	1 - READWRITE

OK Apply Close Reset

Switch Commit Messages

Check this check box to Enable Traps ☒

Figure 37 Enabling the SNMP agent on the Brocade switch

14. Clariion Array and Navisphere

14.1. Introduction

The Clariion Array is a part of the Citigroup's mid tier storage solution. The array can be accessed through the following interfaces:

Access Protocol	Network Protocol	Remarks
Console	None	Serial console. Used for managing the array. Requires physical access to the array.
Console	PPP	Enhanced serial console. Used for managing the array. Requires physical access to the array.
HTTP	TCP/IP	Array initialization (setup)
HTTP	TCP/IP	For downloading Java applet (Navisphere) so that the array can be managed from within a browser such as Internet Explorer
Proprietary	TCP/IP	Between Storage Manager Server and Navisphere
Proprietary	TCP/IP	CLI interface (NaviCLI)
SCSI	FC	Used by hosts to access the storage

The server side of the client-server application that enables management of the array runs on the array service processor and is called the "Storage Management Server". The client side is called "Navisphere Manager" or "Navisphere", and is available as a Java applet that runs within the browser, or a standalone Java application. Additionally, a command line interface ("CLI") tool called the "NaviCLI" is also available, that allows for scripting of common tasks.

The Storage Management Server:

- Receives and responds to requests from Navisphere Manager 6.X
- Forwards requests to the local SP Agents for processing
- Forwards status and configuration updates to Navisphere Manager 6.X
- Replicates user and domain information to all storage systems in domain
- Authenticates user logins and authorizes user requests
- Logs all user logins and actions

14.2. Identification and authentication

Although the Clariion array does identify and authenticate support staff, there are several gaps that are documented in the SAN IS Product TRAM. To compensate, support staff should be first required to authenticate to a SOE server. This is enabled by connecting the array on a private TCP/IP network, and using a dual-homed host to manage it. In addition, if dial-in capabilities are turned on the dual-homed server for vendor access, a firewall must be used to isolate the server from the corporate network. A detailed design of such a network and the required firewall configuration is documented within the GDSE document GDSE-03011-B, "EMC Clariion CX Series Best Practice Guide", available at http://gdse.ny.ssmb.com/GDSE_docs/GDSE-03011-B.pdf under Appendix D.

All Clariion arrays should be made members of a Navisphere security domain at the time of installation. Even if there is only one array on the site, it should be put in a domain. Using management domains enables robust identification of users.

14.3. Authorization and access control

- Access Logix should be installed and enabled on the array at the time of installation. The Access Logix application allows the array to be shared between multiple hosts without compromising confidentiality
- Role based access control is available for managing the array through the Navisphere application. Please see appendix A for a list of available roles
- Role based access control is not available for managing the array through the NaviCLI application. However, users and hosts that can issue NaviCLI commands can be controlled through the "privileged user" configuration. All Clariion Service Processors should be configured with privileged users. This configuration is accessible from the SP properties, "Agent" tab, as shown in figure 35. Each privileged user entry is formatted as <username>@<host IP address>. The "username" is the Windows user name logged onto the management SOE server, and the "IP address" is the IP address of the management SOE server. Please note that this control does not affect access through the Navisphere application.

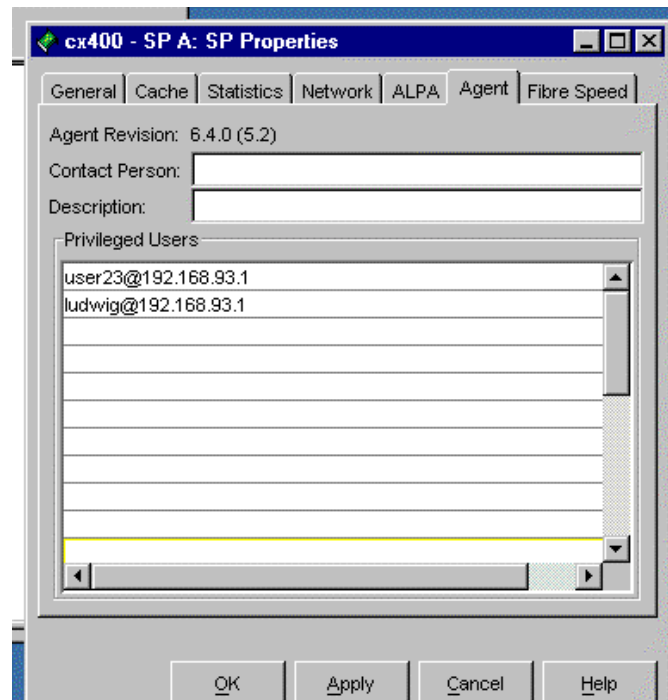


Figure 38 Configuring privileged users on Clariion

Periodic entitlement reviews should be conducted for the above controls.

Further, Storage Management should create level 3 procedures to ensure that passwords are six or more alphanumeric characters, passwords are changed periodically, inactive user accounts are removed and user accounts for users that are no longer responsible for support are removed.

14.4. Confidentiality and Integrity

In order to maintain the confidentiality of business information stored on the array, the following processes should be implemented⁹:

- o Before a disk is returned to the vendor, all information on the disk must be erased
- o Before a logical disk ("LUN") is re-assigned, all information on the LUN must be erased

14.5. Incident detection and response

⁹ Detailed procedures are expected to be available by end of 2004

The Navisphere application collects events into a log from all arrays in the management domain as illustrated in appendix B. The audit log should be archived and periodically reviewed.

14.6. Administration

This component does not initiate, program, process, or authorize business transactions. This product does not internally support segregation of system and security administration or maker/checker functions.

The following default capabilities should be disabled or protected:

- The default setup password for the array should be changed at the time of installation. This is the password that is asked when the following url is accessed:
`http://<array IP address>/setup.htm`
- The default password for the “clariion” user id, which is used from the serial console as well as the SOE management station, should be changed at the time of install
- The default password for the built-in “administrator” user ID within Navisphere should be changed at the time of installation.

15. Remote Fault Management

15.1. Introduction

The fault management of SAN components has been outsourced to the vendor in some locations. The remote management solution allows the vendor to provide round the clock fault monitoring and troubleshooting from a remote location.

A modem is connected to a server that hosts EMC software that provides remote access capability. The public telephone network is used to make the connection.

The remote access capability is enabled by the EMC “OnAlert” application bundle, which consists of the following applications:

- **EMC Dial:** Enables reporting of faults to EMC support center. It is installed on the Connectrix Service Processor, Symmetrix Service Processor and the SOE server hosting the Navisphere application.
- **EMC SymmRemote:** Enables dial-in and remote control of the console. It is usually installed on the Connectrix Service Processor and Symmetrix Service Processor. It can also be installed on the SOE server hosting the Navisphere application.
- **EMC SymmIP:** Secures the dial-in feature of SymmRemote. Once a secured dial-in connection is established with SymmIP, SymmRemote is used for remote control of the console. SymmIP is currently only available for the Symmetrix Service Processor.

Although SAN components can be fully controlled through these remote access solutions, the business information processed and stored on the SAN is not accessible through such solutions.

15.2. Identification and authentication

SymmRemote is not capable of identifying users, or using dynamic tokens for authentication. It supports only one user ID that is used by all vendor support staff.

SymmIP improves on the identification capabilities of SymmRemote by limiting access to hosts installed in the vendor support center by use of digital certificates. Also, because the calls are expected to only originate from the vendor support center, the PBX can be programmed to reject calls coming from all other numbers.

There are several shortcomings with the remote fault management solution, which have been documented in the SAN IS Product TRAM. Improving the fault management process is a challenge because it involves changing processes both on Citigroup and the vendor side¹⁰.

There are configuration settings on the current version of products that can enhance the security, albeit only marginally.

To improve the logon security of SymmRemote, it should be configured as follows:

- SymmIP should be used on the Symmetrix Service Processors for securing the link. Ensure that all Symmetrix Service Processors have SymmIP installed and enabled:
 - o On the Symmetrix Service Processor, click Start, Point to Settings, and click on Control Panel. In the Control Panel window, double-click Add/Remove Programs. In the Add/Remove window, select "SymmIP Enable\Disable\Uninstall" and click on Add/Remove. SymmIP is installed and enabled if the "Disable" radio button is displayed.
 - o On the Symmetrix Service Processor, the "RAS" and "EMC Route Service" Windows services should be set to start automatically.
- In the SymmRemote host's window, select the Settings menu item and then the Logon Security tab.
 - Enable "Make passwords case sensitive"
 - "Time allowed for logging on" should be set to no more than 5 minutes
 - "Logon attempts per call" should not be greater than 5
 - "Disable logons after" should be enabled, and set for no more than 10 failed attempts
 - "Re-enable logons after" should be set to at least 15 minutes
- In the SymmRemote host's window, select the Settings menu item and then the General tab; enable "Strong Authentication"

Further, Storage Management should create level 3 procedures to ensure that passwords are six or more alphanumeric characters, and that passwords are changed periodically.

¹⁰ GDSE has a corrective action plan in place to address these issues

15.3. Authorization and access control

SymmRemote and SymmIP do not have any access control capabilities. In order to restrict access to corporate network resources, the SAN management TCP/IP network must be isolated from the corporate TCP/IP network. This isolation can be achieved in the following ways:

- Having a physically separate, non-routable (“private”) TCP/IP management network for the SAN, with no interconnect to the corporate TCP/IP network.
- Having a routable TCP/IP management network for the SAN that is isolated from the corporate TCP/IP network by a firewall.

The second approach is recommended, because it allows leveraging of corporate network based management frameworks. This topology is illustrated in figure 36.

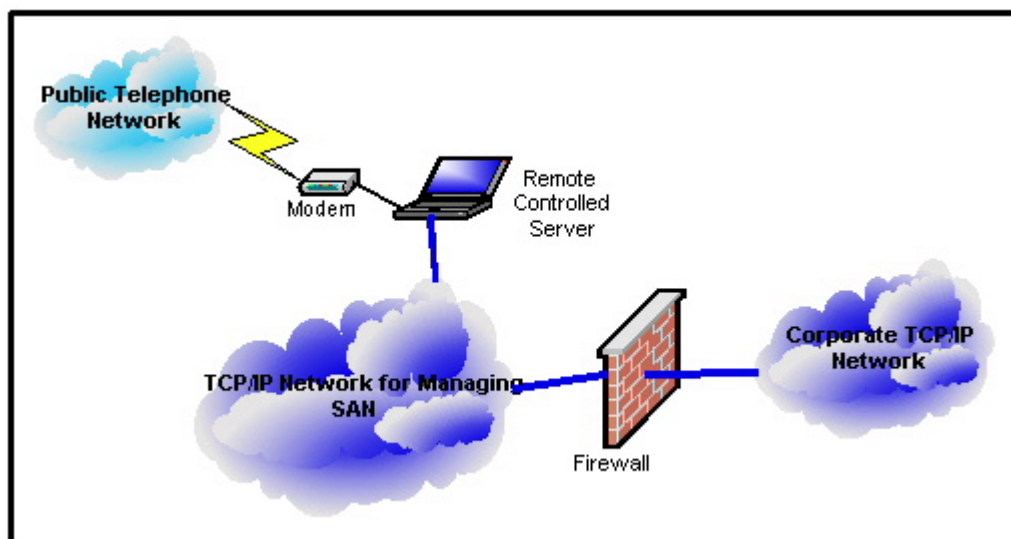


Figure 39 Securing Corporate Network from SAN Network

15.3.1. Vendor Remote Access for Symmetrix

According to a new standard released on December 9, 2004, vendor remote access to the Symmetrix will now go through Citigroup standard dial-in infrastructure called “WWDS” as illustrated in the following figure 40. Please see the “solution design” document from the WWDS engineering web site at http://www.citigroup.net/tie/neteng/external/wwds/EMC_Solution_5.doc.

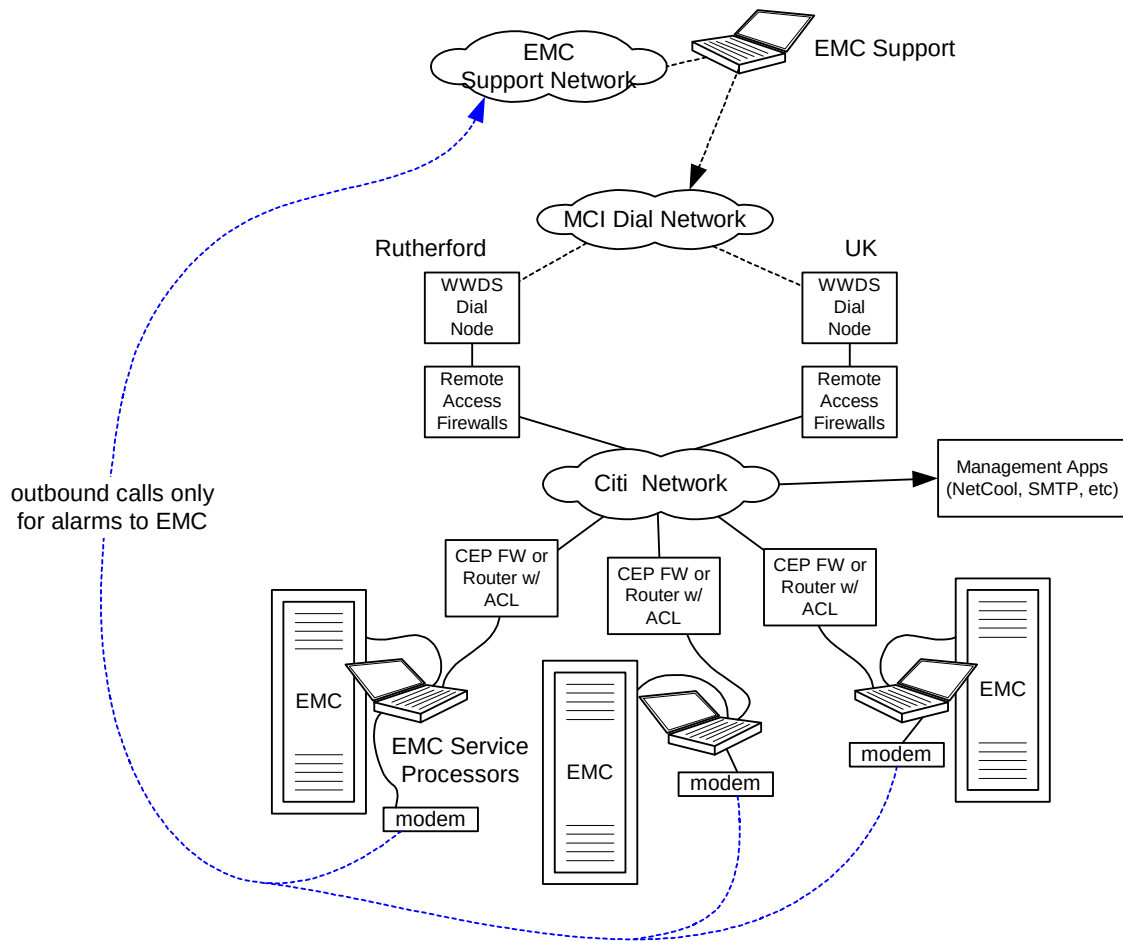


Figure 40 Tactical Solution for Vendor Remote Access to Symmetrix

15.4. Confidentiality and Integrity

The SymmRemote and SymmIP applications do not process any business information. In order to protect passwords, link encryption should be enabled. In the SymmRemote host's window, select the "Settings" menu item and then the "Security" tab; enable "Require data encryption".

15.5. Incident detection and response

The SymmRemote and SymmIP applications track dial-in activity. Logging can be enabled within SymmRemote as following. In the SymmRemote host's window, select the Settings menu item and then the General tab; enable "Log connections and Log file transfers". Logging for the SymmIP application can be enabled with vendor assistance.

Logs should be archived, and should be periodically reviewed.

15.6. Confidentiality and Integrity

The SymmRemote and SymmIP applications do not process any business information. In order to protect passwords, link encryption should be enabled. In the SymmRemote host's window, select the "Settings" menu item and then the "Security" tab; enable "Require data encryption".

15.7. Incident detection and response

The SymmRemote and SymmIP applications track dial-in activity. Logging can be enabled within SymmRemote as following. In the SymmRemote host's window, select the Settings menu item and then the General tab; enable "Log connections and Log file transfers". Logging for the SymmIP application can be enabled with vendor assistance.

Logs should be archived, and should be periodically reviewed.

15.8. Administration

This component does not initiate, program, process, or authorize business transactions. This product does not internally support segregation of system and security administration or maker/checker functions.

The following default capabilities should be disabled or protected:

In the SymmRemote host's window, select the "Settings" menu item and then the "Security" tab.

- Set a "Master Password". Confirm that the password fields are not blank. The master password protects changes to SymmRemote configuration.

16. References

Document	Location
CISS Standards	http://www.citigroup.net/informationsecurityservices/policy/index.htm
GDSE-03011-B, "EMC Clariion CX Series Best Practice Guide"	http://gdse.ny.ssmb.com/GDSE_docs/GDSE-03011-B.pdf

17. Appendices

17.1. Appendix A: Roles within the Navisphere Application

Role	Description
Administrator	The user can access all administrative and management interfaces and data, can change a user's role, can add or delete users, and depending on the scope of the account can add or delete information from a domain.
Manager	The user can view all storage system information and perform storage system operations (such as binding LUNs), but cannot add, modify, or delete user or domain information.
Monitor	The user can view all storage system information, but cannot add, modify, or delete information from a domain or perform configuration operations such as binding LUNs.

17.2. Appendix B: Navisphere Logs

The Navisphere application collects events from all Clariion arrays in the management domain. The events can be reviewed, saved and printed by accessing the “monitors” tab, and selecting “events”. To view events that are Information Security related, the “event code” within the viewer filter should be set to “audit log”. Figure 41 shows a sample of the audit log.

192.168.93.1 - Events								
Line	Date	Time	Event C...	Description	Storage S...	Device	SP	Host
1	3/30/2004	10:56:40 AM	0x4600	'Log In' called by 'admin' on 'Security Service' from client '192.168.93.1' with resu...	N/A	N/A	N/A	emcsrv11
2	3/25/2004	05:39:23 PM	0x4600	'Poll' called by 'admin' on 'APM00040800355' from client '192.168.93.1' with result...	N/A	N/A	N/A	cx500-spa
3	3/25/2004	05:39:20 PM	0x4600	'SetReadCacheState' called by 'admin' on 'APM00040800355' from client '192.16...	N/A	N/A	N/A	cx500-spa
4	3/25/2004	05:39:20 PM	0x4600	'SetWriteCacheState' called by 'admin' on 'APM00040800355' from client '192.16...	N/A	N/A	N/A	cx500-spa
5	3/25/2004	05:39:20 PM	0x4600	'SetReadCacheState' called by 'admin' on 'APM00040800355' from client '192.16...	N/A	N/A	N/A	cx500-spa
6	3/25/2004	05:39:08 PM	0x4600	'Poll' called by 'admin' on 'APM00040800355' from client '192.168.93.1' with result...	N/A	N/A	N/A	cx500-spa
7	3/25/2004	05:39:05 PM	0x4600	'SetMemoryPartitions' called by 'admin' on 'SP B' from client '192.168.93.1' with re...	N/A	N/A	N/A	cx500-spa
8	3/25/2004	05:39:04 PM	0x4600	'SetMemoryPartitions' called by 'admin' on 'SP A' from client '192.168.93.1' with r...	N/A	N/A	N/A	cx500-spa
9	3/25/2004	05:38:06 PM	0x4600	'Poll' called by 'admin' on 'APM00040800355' from client '192.168.93.1' with result...	N/A	N/A	N/A	cx500-spa
10	3/25/2004	05:38:03 PM	0x4600	'SetWriteCacheState' called by 'admin' on 'APM00040800355' from client '192.16...	N/A	N/A	N/A	cx500-spa
11	3/25/2004	05:37:33 PM	0x4600	'Poll' called by 'admin' on 'APM00040800355' from client '192.168.93.1' with result...	N/A	N/A	N/A	cx500-spa
12	3/25/2004	05:37:28 PM	0x4600	'SetMemoryPartitions' called by 'admin' on 'SP B' from client '192.168.93.1' with re...	N/A	N/A	N/A	cx500-spa
13	3/25/2004	05:37:28 PM	0x4600	'SetMemoryPartitions' called by 'admin' on 'SP A' from client '192.168.93.1' with r...	N/A	N/A	N/A	cx500-spa
14	3/25/2004	05:35:36 PM	0x4600	'Log In' called by 'admin' on 'Security Service' from client '192.168.93.1' with resu...	N/A	N/A	N/A	emcsrv11
15	3/25/2004	05:32:13 PM	0x4600	'Poll' called by 'admin' on 'APM00040800355' from client '192.168.93.1' with result...	N/A	N/A	N/A	cx500-spa
16	3/25/2004	05:32:09 PM	0x4600	'SetStatisticsLoggingState' called by 'admin' on 'APM00040800355' from client '19...	N/A	N/A	N/A	cx500-spa
17	3/25/2004	05:32:09 PM	0x4600	'SetStatisticsLoggingState' called by 'admin' on 'APM00040800355' from client '19...	N/A	N/A	N/A	cx500-spa
18	3/25/2004	05:31:42 PM	0x4600	'Log In' called by 'admin' on 'Security Service' from client '192.168.93.1' with resu...	N/A	N/A	N/A	cx500-spa
19	3/25/2004	04:34:31 PM	0x4640	Caller not privileged.	N/A	N/A	N/A	CX500
20	3/25/2004	04:31:50 PM	0x4600	'GetFrontEndspeed' called by 'admin' on 'APM00040800355' from client '192.168....	N/A	N/A	N/A	CX500
21	3/25/2004	04:31:50 PM	0x4600	'GetFrontEndspeed' called by 'admin' on 'APM00040800355' from client '192.168....	N/A	N/A	N/A	CX500
22	3/25/2004	04:31:49 PM	0x4600	'GetAgentRevision' called by 'admin' on '192.168.93.30' from client '192.168.93.1'...	N/A	N/A	N/A	CX500
23	3/25/2004	04:31:23 PM	0x4600	'GetFrontEndspeed' called by 'admin' on 'APM00040800355' from client '192.168....	N/A	N/A	N/A	CX500
24	3/25/2004	04:31:23 PM	0x4600	'GetFrontEndspeed' called by 'admin' on 'APM00040800355' from client '192.168....	N/A	N/A	N/A	CX500
25	3/25/2004	04:31:21 PM	0x4600	'GetAgentRevision' called by 'admin' on '192.168.93.30' from client '192.168.93.1'...	N/A	N/A	N/A	CX500
26	3/25/2004	04:28:35 PM	0x4600	'GetFrontEndspeed' called by 'admin' on 'APM00040800355' from client '192.168....	N/A	N/A	N/A	CX500
27	3/25/2004	04:28:35 PM	0x4600	'GetFrontEndspeed' called by 'admin' on 'APM00040800355' from client '192.168....	N/A	N/A	N/A	CX500

Figure 41 Navisphere Audit Log

17.3. Appendix C: Roles within the Connectrix Manager application

<i>System Administrator</i>	Users can make all control and configuration changes for the Connectrix Manager application. Users with this right can only view configurations and other information in a Product Manager, unless assigned Product Administrator rights as well.
<i>Product Administrator</i>	Users can make control and configuration changes in the Product Manager application. Users with this right can only view configurations and other information in the Connectrix Manager, unless assigned System Administrator rights as well.
<i>Maintenance</i>	Users can perform all control and configuration changes in the Product Manager application, as well as diagnostics, log maintenance, firmware loads, and data collection. Users with this right can only view configurations and other information in the Connectrix Manager unless assigned System Administrator rights as well.
<i>Operator</i>	Users may view status and configuration information in the Product Manager application, and perform operational control changes to the Product Manager such as port blocking and placing the managed product online or offline. Users with this right can only view configurations and other information in the Connectrix Manager unless assigned System Administrator rights as well.
<i>View</i>	Users can view configurations and status, but are unable to make any changes. These rights are the default if no other user rights are assigned.

17.4. Appendix D: Connectrix Manager Logs

The logs on Connectrix Manager are accessible from the Log menu, as illustrated in figure 42.

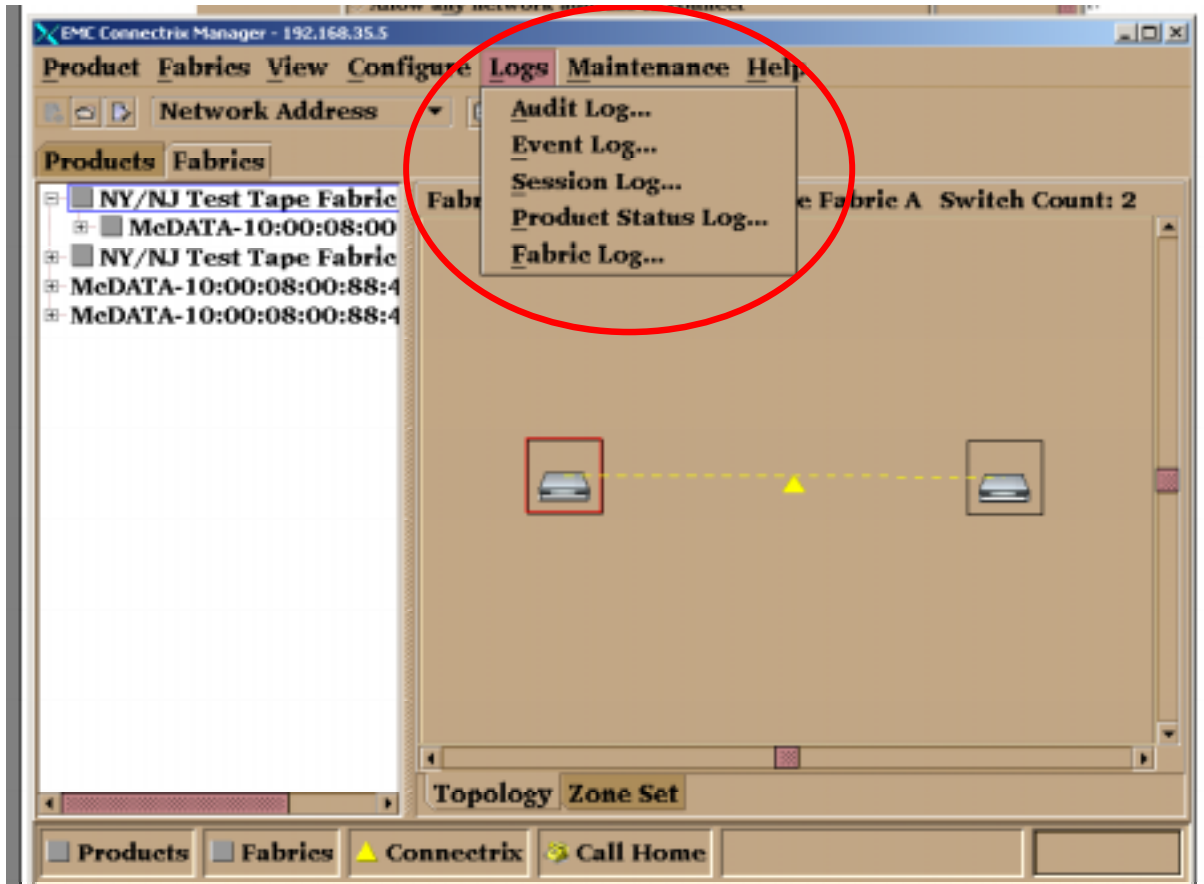


Figure 42 Connectrix Manager Logs

The Audit, Session, Product Status, and Fabric Logs store up to 1000 entries each, and the Event Log stores up to 500 entries. Additional entries overwrite the oldest entries. The most recent entry appears at the top of a log.

From an Information Security perspective, the audit log is the one that is of interest. It displays a history of user actions performed through the Connectrix Manager. Figure 43 shows a sample audit log.

Connectrix Audit Log				
Date/Time	Event	Parameter	Source	
1/23/04 2:37:31 PM	User added	emc	Administrator@192.168.1.1	
11/19/03 3:52:43 PM	Zone Set activated	NJ Director 35R: NJ Test Fabric B	eg55388@192.168.1.1	
11/19/03 3:52:06 PM	Member added to zone	emctest5 b, EMC-50:06:04:82:CC:05:5A:1D	eg55388@192.168.1.1	
11/19/03 3:52:06 PM	Member removed from zone	emctest5 b, EMC-50:06:04:82:CC:05:5A:1C	eg55388@192.168.1.1	
11/19/03 3:40:18 PM	Zone Set activated	NJ Director 34R: NJ Test Fabric A	eg55388@192.168.1.1	
11/19/03 3:39:38 PM	Zone Set activated	NJ Director 35R: NJ Test Fabric B	eg55388@192.168.1.1	
11/19/03 3:15:32 PM	Member added to zone	emctest5 a, EMC-50:06:04:82:CC:05:5A:02	eg55388@192.168.1.1	
11/19/03 3:14:53 PM	Member added to zone	emctest5 b, EMC-50:06:04:82:CC:05:5A:1C	eg55388@192.168.1.1	
11/14/03 10:19:13 AM	Zone Set activated	NJ Director 34R: NJ Test Fabric A	eg55388@192.168.1.1	
11/14/03 10:18:28 AM	Zone Set activated	NJ Director 35R: NJ Test Fabric B	eg55388@192.168.1.1	
11/14/03 10:17:42 AM	Member added to zone	emctest03 B DMX584 FA14B0 B, EMC-50:06:04:82:CC:05:5A:1C	eg55388@192.168.1.1	
11/14/03 10:16:51 AM	Member added to zone	emctest03 A DMX584 FA03A0 A, EMC-50:06:04:82:CC:05:5A:03	eg55388@192.168.1.1	
11/12/03 3:05:45 PM	Zone Set activated	NJ Director 34R: NJ Test Fabric A	eg55388@192.168.1.1	
11/12/03 3:04:27 PM	Member removed from zone	emctest03 B DMX584 FA14B0 B, EMC-50:06:04:82:CC:05:5A:1C	eg55388@192.168.1.1	
11/12/03 3:04:00 PM	Member removed from zone	emctest03 A DMX584 FA03A0 A, EMC-50:06:04:82:CC:05:5A:03	eg55388@192.168.1.1	
11/4/03 1:20:48 PM	Zone Set activated	NJ Director 34R: NJ Test Fabric A	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone removed from zone set	NY-NJ-SRDF-TEST bkup1002, S0624 sanad3 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone removed from zone set	NY-NJ-SRDF-TEST, S0624 sanad3 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone deleted	S0624 sanad3 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone removed from zone set	NY-NJ-SRDF-TEST bkup1002, S0624 intps4 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone removed from zone set	NY-NJ-SRDF-TEST, S0624 intps4 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone deleted	S0624 intps4 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone removed from zone set	NY-NJ-SRDF-TEST bkup1002, S0624 intps3 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone removed from zone set	NY-NJ-SRDF-TEST, S0624 intps3 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone deleted	S0624 intps3 a	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone removed from zone set	NY-NJ-SRDF-TEST bkup1002, S0624 emctest0 b-1	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone removed from zone set	NY-NJ-SRDF-TEST, S0624 emctest0 b-1	ld59486@192.168.1.1	
11/4/03 12:31:33 PM	Zone deleted	S0624 emctest0 b-1	ld59486@192.168.1.1	

Figure 43 Connectrix Manager Audit Log

- The Date/Time column logs the date and time that the logged event took place
- The Event column describes the action that took place. Logged actions can include:
 - o Defining a new product
 - o Modifying product attributes
 - o Deleting product definitions
 - o Defining a new user
 - o Modifying user administration
 - o Deleting user administration
 - o Creating a zone set
 - o Modifying a zone set
 - o Modifying SNMP options
- The Parameter column describes the parameter affected by the event. For example, if a product is added or deleted, the product's network address is displayed.
- The Source column identifies the workstation from which the user performed the logged action. If the change was made locally from the Connectrix service processor, the Connectrix service processor address appears. If the Source column contains EmcBridge@<IP address>, that means the action was initiated by either EMC FibreZone or EMC ECC application.

17.5. Appendix E: Symmetrix Array Logs

Sample output from the ***symaudit -sid <sid> list -v*** command:

Record Number : 309
Records in Seq : 2
Offset in Seq : 2
Time : 03/26/04 10:29:03
Vendor ID : EMC Corp
Application ID : ECC
Application Version : 5.1.0.0
API Library : SEK
API Version : V5.4.0.0 (Edit Level: 532)
Host Name : ECCTEST03AS
OS Name : WinNT
OS Revision : 5.0.2195Se
Client Host :
Process ID : 00001832
Task ID : 00002584
Function Class : DEVMask
Action Code : Add
Text : [0031 0091 0099]

Record Number : 310
Records in Seq : 2
Offset in Seq : 1
Time : 03/26/04 10:29:07
Vendor ID : EMC Corp
Application ID : ECC
Application Version : 5.1.0.0
API Library : SEK
API Version : V5.4.0.0 (Edit Level: 532)
Host Name : ECCTEST03AS
OS Name : WinNT
OS Revision : 5.0.2195Se
Client Host :
Process ID : 00001832
Task ID : 00002584
Function Class : DEVMask
Action Code : Add
Text : Added the following devices to the device masking data
base for Symmetrix 000387430127 by WWN 200000e069c01490 for director 35
for port 0

17.6. Appendix F: Brocade switch logs

Kiwi Syslog Daemon (Version 7.1.0)				
File View Help				
Display 00 (Default)				
Date	Time	Priority	Hostname	Message
04-13-2004	17:29:51	Local7.Warning	192.168.93.21	<010>
04-13-2004	17:29:51	Local7.Warning	192.168.93.21	WARNING FW-BELOW, 3, fopportState014 (FOP Port State Changes 14) is below low boundary. current value : 0 Change(s)/minute. [normal]
04-13-2004	17:29:51	Local7.Warning	192.168.93.21	14 0x101278f0 (tThad): Apr 13 13:51:13
04-13-2004	17:29:49	Local7.Warning	192.168.93.21	<010>
04-13-2004	17:29:49	Local7.Warning	192.168.93.21	WARNING FW-BELOW, 3, fopportState015 (FOP Port State Changes 15) is below low boundary. current value : 0 Change(s)/minute. [normal]
04-13-2004	17:29:49	Local7.Warning	192.168.93.21	13 0x101278f0 (tThad): Apr 13 13:51:11
04-13-2004	17:28:49	Local7.Warning	192.168.93.21	<010>
04-13-2004	17:28:49	Local7.Warning	192.168.93.21	WARNING FW-ABOVE, 3, fopportState014 (FOP Port State Changes 14) is above high boundary. current value : 4 Change(s)/minute. [faulty]
04-13-2004	17:28:49	Local7.Warning	192.168.93.21	12 0x101278f0 (tThad): Apr 13 13:50:11
04-13-2004	17:28:47	Local7.Warning	192.168.93.21	<010>
04-13-2004	17:28:47	Local7.Warning	192.168.93.21	WARNING FW-ABOVE, 3, fopportState015 (FOP Port State Changes 15) is above high boundary. current value : 4 Change(s)/minute. [faulty]
04-13-2004	17:28:47	Local7.Warning	192.168.93.21	11 0x101278f0 (tThad): Apr 13 13:50:08
04-13-2004	17:28:35	Local7.Warning	192.168.93.21	<010>
04-13-2004	17:28:35	Local7.Warning	192.168.93.21	WARNING FW-STATUS_SWITCH, 3, Switch status changed from Marginal/Warning to HEALTHY/OK
04-13-2004	17:28:35	Local7.Warning	192.168.93.21	10 0x101278f0 (tThad): Apr 13 13:49:57
04-13-2004	17:28:35	Local7.Info	192.168.93.21	<010>
04-13-2004	17:28:35	Local7.Info	192.168.93.21	INFO TRACK-CONFIG_CHANGE, 4, Config file change from task:tHttp9
04-13-2004	17:28:35	Local7.Info	192.168.93.21	9 0x10d325d0 (tHttp9): Apr 13 13:49:57
04-13-2004	17:28:32	Local7.Warning	192.168.93.21	<010>
04-13-2004	17:28:32	Local7.Warning	192.168.93.21	WARNING FW-STATUS_SWITCH, 3, Switch status changed from HEALTHY/OK to Marginal/Warning
04-13-2004	17:28:32	Local7.Warning	192.168.93.21	8 0x101278f0 (tThad): Apr 13 13:49:54
04-13-2004	17:28:31	Local7.Info	192.168.93.21	<010>
04-13-2004	17:28:31	Local7.Info	192.168.93.21	INFO TRACK-CONFIG_CHANGE, 4, Config file change from task:tHttp9
04-13-2004	17:28:31	Local7.Info	192.168.93.21	7 0x10d325d0 (tHttp9): Apr 13 13:49:53
04-13-2004	17:23:11	Local7.Info	192.168.93.21	<010>
04-13-2004	17:23:11	Local7.Info	192.168.93.21	INFO TRACK-FAILED_LOGIN, 4, Unsuccessful login
04-13-2004	17:23:11	Local7.Info	192.168.93.21	6 0x101ef0c0 (tShell): Apr 13 13:44:33
04-13-2004	17:23:04	Local7.Info	192.168.93.21	<010>
04-13-2004	17:23:04	Local7.Info	192.168.93.21	INFO TRACK-LOGOUT, 4, Logout
04-13-2004	17:23:04	Local7.Info	192.168.93.21	5 0x101ef0c0 (tShell): Apr 13 13:44:26
04-13-2004	17:21:16	Local7.Info	192.168.93.21	<010>
04-13-2004	17:21:16	Local7.Info	192.168.93.21	INFO TRACK-CONFIG_CHANGE, 4, Config file change from task:tShell
04-13-2004	17:21:16	Local7.Info	192.168.93.21	4 0x101ef0c0 (tShell): Apr 13 13:42:38
04-13-2004	17:20:28	Local7.Info	192.168.93.21	<010>
04-13-2004	17:20:28	Local7.Info	192.168.93.21	INFO TRACK-LOGIN, 4, Successful login
100% 39 MPH 17:30 04-13-2004				

Figure 44 Brocade switch logs collected on a syslog server

SNMP Trap Watcher			
File Edit Settings			
Time	Date	Source	Description
17:36:10	04/13/2004	192.168.93.21	0x101278f0 (iThad) FW-ABOVE fopportState015 (FOP Port State Changes 15) is above high boundary. current value : 4 Change(s)/minute. (faulty)
17:36:10	04/13/2004	192.168.93.21	Apr 13 13:57:32 0x101278f0 (iThad) FW-ABOVE fopportState015 (FOP Port State Changes 15) is above high boundary. current value : 4 Change(s)/minute. (...)
17:36:10	04/13/2004	192.168.93.21	0x101278f0 (iThad) FW-ABOVE fopportState014 (FOP Port State Changes 14) is above high boundary. current value : 4 Change(s)/minute. (faulty)
17:36:10	04/13/2004	192.168.93.21	Apr 13 13:57:32 0x101278f0 (iThad) FW-ABOVE fopportState014 (FOP Port State Changes 14) is above high boundary. current value : 4 Change(s)/minute. (...)
17:36:09	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:36:09	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:36:09	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:36:09	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:59	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:59	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:59	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:59	04/13/2004	192.168.93.21	0x101278f0 (iThad) FW-STATUS_SWITCH Switch status changed from Marginal/Warning to HEALTHY/OK
17:35:59	04/13/2004	192.168.93.21	Apr 13 13:57:21 0x101278f0 (iThad) FW-STATUS_SWITCH Switch status changed from Marginal/Warning to HEALTHY/OK
17:35:58	04/13/2004	192.168.93.21	Config file change from task:iHttp1
17:35:58	04/13/2004	192.168.93.21	0x10d325d0 (iHttp1) TRACK-CONFIG_CHANGE Config file change from task:iHttp1
17:35:58	04/13/2004	192.168.93.21	Apr 13 13:57:20 0x10d325d0 (iHttp1) TRACK-CONFIG_CHANGE Config file change from task:iHttp1
17:35:56	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:56	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:56	04/13/2004	192.168.93.21	0x101278f0 (iThad) FW-STATUS_SWITCH Switch status changed from HEALTHY/OK to Marginal/Warning
17:35:56	04/13/2004	192.168.93.21	Apr 13 13:57:18 0x101278f0 (iThad) FW-STATUS_SWITCH Switch status changed from HEALTHY/OK to Marginal/Warning
17:35:56	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:56	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:56	04/13/2004	192.168.93.21	Trap contains no readable strings.
17:35:22	04/13/2004	Local	Trap Watcher Started - listening on UDP port 162.

Traps Received: 23

17:36:47

Figure 45 Brocade switch logs collected on a SNMP management station

17.7. Appendix G: Citigroup Information Security Standards

Please visit the Information Security Services website for the current version.

- 1.1 Businesses will designate Information Owners, in writing, for Citigroup Information under their control.
- 1.2 The Information Owner will classify Citigroup Information under their control as one of the following Information Classifications: RESTRICTED, HIGHLY CONFIDENTIAL, CONFIDENTIAL, INTERNAL, PUBLIC.
 - 1.3.1 Each business will identify the Criticality of each Significant Information System or Process managed by the business.
 - 1.3.2 Each business will identify instances where the Information System or Process does not comply with the ISP&S.
 - 1.3.3 Each business will identify the people, process and technology vulnerabilities that could cause the Information System or Process to be compromised, damaged, tampered with, or otherwise impaired.
 - 1.3.4 Each business will identify appropriate threat scenarios based on these vulnerabilities and instances of non-compliance to document the various inherent risks to the asset.
 - 1.3.5 Each business will identify security action plans to mitigate the risk associated with instances of non-compliance or with Information Systems or Processes identified as High or Medium Risk.
- 1.4 Each business will follow the information security risk management process and forms specified by the ISLC.
- 1.5 Based upon the assessment process and the classification of information, the business will specify the level of security required to protect this information and ensure that sufficient controls are in place to achieve the specified level.
- 1.6 Each business will ensure that an inventory is maintained of all Information Systems and Processes under their control. The inventory will specifically identify the Information Owner, Information Classification, Criticality level, Risk level and Infrastructure Security Classification.
 - 1.7.1 Each Technology Manager (TM), working with their designated Citigroup engineering and operations groups, must ensure that the Infrastructure Security Classifications for their environments are specified and documented.
 - 1.7.2 Each Technology Manager (TM), working with their designated Citigroup engineering and operations groups, must ensure that the Citigroup Infrastructure managed by the TM meets or exceeds the Class C Infrastructure Security Classification.
 - 1.7.3 Each Technology Manager (TM), working with their designated Citigroup engineering and operations groups, must ensure that the infrastructure of any business that is connected to the Citigroup Infrastructure managed by the TM meets or exceeds the Class C Infrastructure Security Classification (any network that does not meet the minimal classification requirements must either be logically partitioned from the Citigroup network, or physically disconnected).
 - 1.7.4 Each Technology Manager (TM), working with their designated Citigroup engineering and operations groups, must ensure that appropriate working practices to achieve compliance with the ISP&S are implemented.
- 2.1 All Citigroup technology platforms will authenticate the identity of users (including other systems accessing these platforms) prior to initiating a session or transaction, unless the user is entitled only to read INTERNAL or PUBLIC data on these platforms.
 - 2.2.1 All users will be identified to the technology platform by a unique User ID.
 - 2.2.2 All users will be identified to the technology platform by a method of authentication enabling unique identification of the user e.g., a static or dynamic password, public key, biometric or other authentication mechanism.
- 2.3 Users are accountable for all activity associated with their User ID and password.
 - 2.4.1 Static passwords will never be shared, made known to others or written down.
 - 2.4.2 Static passwords will never be displayed on the screen in clear text (with the exception of one time use password resets).

- 2.5 Static passwords (other than PINs) will consist of a minimum of six (6) alphabetic and numeric characters.
- 2.6 PINs may be used as the sole method of authentication to access Information Systems only if the PINs are; required by local laws or regulations or by rules adopted by self-regulatory bodies (for example, central banks or payment associations with which Citigroup is associated), necessary to meet physical device constraints (for example, keypad, telephone, smart card), used for Medium or Low Criticality consumer applications.
- 2.7 User IDs associated with a static password must be disabled after not more than six (6) consecutive failed login attempts.
- 2.8 The business will implement a documented process to ensure that all static passwords are changed on a periodic basis and that User IDs are disabled after a stated period of inactivity. The periods selected will be commensurate with the criticality of the Information System. The business may waive the requirement for changing static passwords and disabling User ID's for customer access to Information Systems, provided that the business periodically reminds its customers that manually changing their passwords provides greater security.
- 2.9 Dynamic passwords or digital certificates will be used for non-customer remote access to the Citigroup global network and for administrative access to routers and firewalls.
- 2.10 Information Systems that use dynamic passwords or digital certificates will use ISLC approved authentication services to validate the password or certificate.
- 2.11 Functional IDs are exempted from the restriction on sharing passwords, the requirements for a unique User ID, the disabling of passwords after six (6) failed attempts and the periodic changing of passwords.
- 3.1.1 Businesses will implement access controls that are fully documented.
- 3.1.2 Businesses will implement access controls that are auditable.
- 3.1.3 Businesses will implement access controls that ensure that users are given only those privileges and entitlements necessary to perform their function.
- 3.2 Where access controls are not possible or are prohibitive control may be implemented through the use of audit trails and reconciliation processes.
- 3.3 Businesses will protect all Information Systems and Processes from unauthorized access and will secure them using security products, functions or processes commensurate with the Criticality of the Information System or Process, the Information Classification and the Infrastructure Security Classification. This requirement includes non-production environments such as test and development systems.
- 3.4 Access entitlements will be traceable to the User ID and assigned owner.
- 3.5 The business will implement a documented process to review and verify user entitlements at least semi-annually.
- 3.6 The business/technology manager will document and implement a process to ensure access rights reflect changes in employee and External Provider status.
- 3.6.1 Each business/technology manager shall be responsible for the access rights of employees and external providers under their control. Required changes to issued access rights due to transfers and changes in job functions shall be formally communicated to the security administration function within 24 hours. The communication shall identify the access rights that need to be amended and the actual date when they are to be amended.
- 3.6.2 Managers must notify security administration within 24 hours of employees or External Provider no longer working for Citigroup.
- 3.6.3 Access rights will be changed by the security administration function within 7 days of being notified of a change.
- 3.6.4 Notification to the security administration function and subsequent changes to access rights must be completed in Class A+ infrastructures before the employee or External Provider is notified of the change in status.
- 3.7 The Legal Department approved banner text, when supported by the operating system or application, will be displayed at all system entry points where a user initially signs on.
- 3.8 Remote access to Information Systems will be protected from unauthorized use. In particular, all remote access is prohibited on any Information System connected to the Citigroup global network, except (A) over ISLC approved remote access systems or (B) where documented and explicitly approved in writing by the business head, the Business Information Security Officer and the Technology Manager and either the Technical Information Security Officer for remote access to Class C Infrastructure or the Senior Security Officer for remote access to Citigroup Infrastructure classified higher than Class C.

3.9 Confidential, Highly Confidential and Restricted Information must only be stored on Citigroup owned and managed devices or on vendor owned devices that are subject to a contract that is compliant with Citigroup policies and standards.

3.10 If a business permits employees to access the Citigroup global network remotely from home PC's or other employee owned devices, the business must communicate to each employee that access must be conducted only over ISLC approved remote access systems.

3.11.1 Unless approved in writing by the Senior Security Officer, the business will take appropriate steps (including technical solutions and training and awareness programs) to ensure that wireless local area networks (WLAN's) and other wireless devices must not be connected to the Citigroup global network.

3.11.2 Unless approved in writing by the Senior Security Officer, the business will take appropriate steps (including technical solutions and training and awareness programs) to ensure that employees do not access external Internet email accounts from the Citigroup global network.

3.11.3 Unless approved in writing by the Senior Security Officer, the business will take appropriate steps (including technical solutions and training and awareness programs) to ensure that employees do not use instant messaging, peer-to-peer networks or other Internet collaborative tools to transmit or store Citigroup Information beyond the Citigroup global network.

3.12.1 The business, as part of its periodic employee information security awareness program, will ensure its employees are aware of and understand that the use of home or public WLAN's for remote access to the Citigroup global network is not permitted unless the remote connection is made through a virtual private network (VPN).

3.12.2 The business, as part of its periodic employee information security awareness program, will ensure its employees are aware of and understand that only Public and Internal Information may be stored on employee owned devices (for example, home computers, personal digital assistants, mobile Internet and email appliances, etc.).

3.13 The business shall be responsible for the network connections under their control and will document a procedure to inform their technology support function within 24 hours of network connections becoming inactive.

3.14.1 Technology support functions will disable inactive connections within twenty-four hours of formal notification from the business if the connection is in an area accessible by the public.

3.14.2 Technology support functions will disable inactive connections within seven days of formal notification for connections that are not assigned to any individual and that are located in unlocked offices, common areas, conference rooms and other locations where the business does not restrict access.

3.14.3 Technology support functions will disable inactive connections within thirty days of notification for any connection assigned to a specific individual.

3.15 Only Citigroup owned and managed devices or vendor devices that comply with these Standards and are supervised and authorized by the business may have direct access to the Citigroup global network.

4.1 Businesses will inform all users of Information Systems or Processes (in particular e-mail and voice mail system users) that all information stored, transmitted or handled by these systems or processes is the property of Citigroup and that this information may be reviewed and monitored for administrative, security and other lawful purposes.

4.2 Businesses will protect Citigroup Information regardless of the media upon which it is maintained. This Standard applies, but is not limited to, the following types of media upon which information is contained, recorded or stored: cards, cassette, CD, check stock, diskette, hard copy output, magnetic disk, magnetic tape, microfilm, microfiche, optical disk or paper documents.

4.3 Subject to the exclusions specified in Appendix A, all Citigroup Information that is stored or transmitted in an electronic format will be encrypted. If encryption is not required, the business must still protect the Citigroup Information from unauthorized access.

4.4 Each business unit will develop, document and enforce a clear desk program that protects all RESTRICTED, HIGHLY CONFIDENTIAL and CONFIDENTIAL information stored on any media from unauthorized access.

4.5 RESTRICTED, HIGHLY CONFIDENTIAL and CONFIDENTIAL information at the point at which the information is no longer useful to the business plus any additional period of retention required by law, regulation or contract will be destroyed in a manner commensurate with the level of threat to the information.

4.6 ISLC approved anti-virus products will be installed, updated and maintained on all personal computers and on all LAN servers, mail servers and other devices that store content received from external sources (provided that an ISLC approved anti-virus product is available for the device).

4.7.1 Businesses/technology will only run operating systems and software that are currently supported by an approved vendor or have an active and appropriate release of patches and configuration updates available to address security issues,

4.7.2 Businesses/technology will apply all approved security patches and configurations within the time periods specified by the Vulnerability Threat Management Process.

4.8 Each business shall ensure that External Providers that process, manage or access Confidential, Highly Confidential or Restricted Information comply with the applicable sections of the Citigroup Information Security Standards, and the business' information security practices and procedures. For those External Providers that process, manage or access Internal or Public Information, compliance may be achieved through the use of a Citigroup legal counsel approved non-disclosure agreement or other provisions that limits disclosure of the information to authorized parties.

5.1 Business management in conjunction with Compliance, Information Security, Corporate Security and any other relevant security functions, will develop, document and ensure compliance with the Citigroup Information Security Office (CISO) Security Incident Response Team (SIRT) process.

5.2.1 Businesses will ensure that all Information Systems that store Citigroup Information use audit trails to log and report all attempted violations of system security. The level of audit trail reporting shall be commensurate with the Criticality of the Information System.

5.2.2 Businesses will ensure that all Information Systems that store Citigroup Information use audit trails to log and report all significant events relating to security and system administration, financial transactions and customer information. The level of audit trail reporting shall be commensurate with the Criticality of the Information System.

5.3 Businesses will ensure that audit trails are reviewed on a periodic basis that is commensurate with the Criticality of the Information System. Any suspicious activity shall be acted upon immediately. The review process must be segregated to ensure the reviewers do not review their own activity.

6.1 Businesses will ensure that appropriate background and reference checks are performed on all Citigroup staff (that is, job applicants who have accepted a job offer and External Providers) who perform security-related functions or who are granted highly privileged access (for example, system administration, database administration, change control or supervisor status) to Citigroup Information.

6.2 Each business will incorporate an Information Security Review Process into their processes and procedures for the selection, development and implementation of applications, products and services in order to ensure compliance with these Standards.

6.3 Any individual assigned to the role of Information Security Administration must not perform transactions that conflict with this role. Specifically, they must not initiate, program, process or authorize business transactions.

6.4.1 Commensurate with the criticality of the Information System, systems administration and security administration functions must be segregated to provide separation of duties for the same system.

6.4.2 Commensurate with the criticality of the Information System, administrative actions (for example, adding/deleting users, changes to entitlements/ passwords) require an independent verification or maker/checker process.

6.5 The Information Security Administration function must not be outsourced unless approved by the business head and their ISLC representative.

6.5.1 If the Information Security Administration function is outsourced, a documented process must be implemented to manage vendor activity in compliance with the Citigroup policies and standards.

6.6 Each business will implement a process to ensure that all security functions, products, tools and services are configured to meet these Standards and that all default access capabilities are removed, disabled or protected to prevent their unauthorized use.

6.7.1 At least annually, each business shall review its information security practices and procedures for compliance with the Information Security section of the CITMP and these Standards. The review will assess the adequacy of these practices and procedures based on changes in their processes, technology, business responsibilities, the sensitivity of customer or corporate information and the risks that may threaten this information.

6.7.2 At least annually, each business shall review whether any Compliance Questionnaires, Information or Infrastructure Security Classifications, Criticality Assessments or Residual Risk forms (including Threat Scenario Forms) should be modified based on such changes.

7.1 Each business shall develop and ensure that all employees, contractors, and temporary staff that are new to Citigroup or who have a significant change in job responsibility, receive training on the information security related aspects of their job function within 90 days of their hire date.

7.2.1 Each business shall ensure that all employees, contractors, and temporary staff who are web software developers, customer service staff or information security officers attend annually a ISLC sponsored or approved Information Security training program specific to their function.

7.2.2 Each business shall ensure that all employees, contractors, and temporary staff who are systems administrators and security administrators, who manage or support Citigroup information systems, receive an ISLC approved training course at least every 36 months.

7.3.1 Each business shall ensure that all employees, contractors, and temporary staff annually view an ISLC sponsored or approved IS Overview Webcast, Employee Guide, video or other material on Information Security.

7.3.2 Each business shall ensure that all employees, contractors, and temporary staff annually receive business developed awareness material on the information security related aspects of their job function.

8.1.1 All businesses will ensure that all Citigroup products, services or applications, which use the Internet for connectivity or communications undergo an independent ethical hack prior to the application or system going live.

8.1.2 All businesses will ensure that all Citigroup products, services or applications, which use the Internet for connectivity or communications undergo a Vulnerability Assessment using security testing processes approved by the ISLC whenever updates are introduced into the production environment.

8.2 All High Criticality Internet Applications will receive two Vulnerability Assessments annually, of which one will be an independent ethical hack.

8.3 All Medium and Low Criticality Internet Applications will receive an annual Vulnerability Assessment.

8.4 Managers of technology infrastructures will ensure that an annual Vulnerability Assessment of their technical infrastructure is performed.

8.5 High-risk findings identified in the Vulnerability Assessment will be resolved before the product, service or application can go live or updates introduced into the production environment. The application or systems manager will maintain a record of all actions taken to resolve the high-risk findings.

9.1 Businesses will ensure that all Information Systems use only ISLC approved Cryptographic algorithms, key lengths, key management and Security protocols.

9.2 Businesses utilizing digital certificates and public key technologies will utilize internal Certificate Authorities or ISLC approved external Certificate Authorities.

10.1.1 Businesses responsible for managing or maintaining internal Citigroup networks will ensure that all external Internet Protocol (IP) connections to the Citigroup global network are protected by a firewall.

10.1.2 Businesses responsible for managing or maintaining internal Citigroup networks will ensure that all external Internet connections to the Citigroup global network are monitored by a real-time intrusion detection system.

10.2 Only ISLC approved firewalls, intrusion detection systems and security service providers may be used.

10.3 All configuration changes to Firewalls and IDS systems must be implemented through approved CITMP change control mechanisms.

10.4 Firewalls must be configured with a default "deny all" rule.

10.5 When a suspicious Security Events occurs, a SIRT response must be generated and escalated through the defined SIRT process and procedure.

10.6 All system alarms associated with a Firewall or IDS generated Security Event must be logged and archived daily.

10.7 Citigroup Firewalls and Intrusion Detection System management must have the capability to respond to a Security Event within 15 minutes of their occurrence 24hour by 7days per week.