

CITIGROUP TECHNOLOGY INFRASTRUCTURE (ASIA PACIFIC)

STORAGE ENGINEERING

LEVEL 3 TECHNICAL DOCUMENT

SG-CTI-SAN SECURE BUILD IMPLEMENTATION

PROJECT ID	:	NSR 2005/1026
SPONSORING BUSINESS	:	CTI
PREPARED BY	:	Sampath Kumar, Suresh Kumar
VERSION	:	2.0

CHANGE HISTORY

ITEM NO	SECTION AMENDED	AMENDED BY	AMENDMENT DATE	VERSION NO.	DESCRIPTION OF THE CHANGE
1	New Document	Sampath Kumar	05-May-2006	1.0	Request for review
2	All	Sampath Kumar	24-May-2006	2.0	Final release after review



APPROVALS

LEVEL 3 TECHNICAL DESIGN DOCUMENT FOR SG-CTI-SAN SECURE BUILD IMPLEMENTATION

PREPARED BY:

Sampath Kumar
Storage Engineering

Date

Suresh Kumar
Storage Engineering

Date

REVIEWED BY:

Fibish Madathil
Storage Engineering

Date

Geok-Kwee, Tee
CTI Engineering Storage - Domain Manager

Date

Khoon-Chiang, Loo
Storage Integration - Domain Manager

Date

Borromeo, Raymond
Storage Integration - Unit Manager

Date

Theng-Wee, Heng
Storage Operations - Domain Manager

Date

Krishnakumar, Pazhore
Storage Operations - Unit Manager

Date

Lee, Joseph Cp
BISO

Date

Smith, Chris
CTI Engineering WinTel - Domain Manager

Date

Kan, Philip
CTI Engineering WISE – Domain Manager

Date

Bhatia, Mayank
Project Manager

Date

SCOPE

The primary scope of this project is to implement Secure Build for different sub-systems in the APPC SAN infrastructure. The scope specific to Storage Engineering covers the following:

- Design of infrastructure in compliance with applicable global guidelines for Log consolidation, SANScreen, SANTegrity, Solutions Enabler in Solaris and Management server (for Connectrix, HDS and Clariion management)
- Perform a POC for the functionality of above-mentioned initiatives.

OUT OF SCOPE*

- Design of supporting infrastructure for the secure build e.g setup of eTrust Audit servers.
- Definition of operation processes.
- Definition of Entitlement process.

ASSUMPTIONS

- Etrust Audit servers would be ready on time to facilitate the storage sub-system clients.
- The sub-systems under scheduled upgrade or technology refresh would not be considered for the secure build.
- Necessary firewall ports will be opened (Details provided in Appendix A).
- Only Fabric and port binding are considered for SANTegrity deployment as per global guidelines.
- BCV groups / batch jobs involved in regional flex cube, Japan flex cube, HA servers and remote backup servers will not be moved to new Solaris SE server.
- SYMACL will be implemented after successful migration of SE to solaris in phases.
- SYMACL implementation would restrict the existing HP-UX SE servers to do BCV management.
- All project streams need to complete their assigned work and interdependencies of the project are closed.
- HDS sub-systems other than TagmaStore will not require any remote management.
- Guidelines mentioned in global documents would be used for sub-systems, which do not have a secure build.

* This is a general definition. Items in scope and out of scope for individual modules have been mentioned under their respective sections

RISKS

RISK DESCRIPTION	RISK CATEGORY	PRIORITY	RESPONSIBLE RESOURCE	MITIGATION STRATEGY
APPC personnel have no prior experience in deploying the initiatives	Schedule	M	All Storage Streams	Vendor provided trainings could be used

ISSUES

ISSUE DESCRIPTION	ISSUE CATEGORY	PRIORITY	RESPONSIBLE RESOURCE	ACTION PLAN
Proposed number of ETrust Audit client licenses has to be informed to ELA before implementation	Cost	M	Storage Operations	To be informed to global ELA as scheduled.
HDS log collection has to be done manually till Global inform about automated log collection procedure.	Resource	L	GDSE / Storage Operations	To implement automated log transfer once designed by global.
HDS microcode level should be upgraded to minimum 50-04-47-00/00 for log collection to happen.	Schedule	H	Storage Operations	Need to schedule the upgrade to meet the timelines.
eTrust does not support symm 4.8 or microcode 5567 to send the logs	Cost, Resource	L	Storage Operations	Microcode needs to be updated
The policy ownership, retention policy and log review process should be addressed before the production rollout.	Resource	M	Storage Operations / ISA	Finalise on the roles and responsibilities.
HiCommand Device Manager license is required for all HDS subsystems to work with SANScreen	Cost	M	Storage Operations	Have to confirm and procure the licenses for sub-systems which require DM.
Clariion alerting for a site cannot happen if management server is down at that site.	Schedule, Resource	L	Storage Operations	Alerting feature to be configured manually on the stand-by server.
All Clariion sub-systems have to be scheduled to get connected to the storage private IP network to do management & log collection	Schedule, Resource	M	Storage Operations	Need to schedule the connectivity to meet the timelines.

SCHEDULE AND MILESTONES

MILESTONES	DUE DATE	RESOURCE / TEAM INVOLVEMENT	DEPENDENCY
Project Kick-Off	04-Jan-2006	All Streams	
POC Initiation	01-Feb-2006	Storage Engineering	Storage Operations
Project POC complete	14-Apr-2006	Storage Engineering	
L3 Document Complete	04-May-2006	Storage Engineering	
PDD Approval	22-May-2006	Project Management	
UAT setup Start	28-Mar-2006	Storage Integration	
UAT setup Complete	06-Aug-2006	Storage Integration	
Production setup Start	28-Apr-2006	Storage Operations	
Production setup Complete	28-Aug-2006	Storage Operations	
Build & Handover	23-Oct-2006	Storage Streams	
Project Closure	18-Dec-2006	All Streams	

DETAIL SCHEDULE (MS PROJECT PLAN)

Please see detailed project plan attached in Appendix B.

OPERATION IMPACT**RESOURCE & SKILL-SET**

Operations personnel have been detailed on the skills required for daily management of the infrastructure.

TRAINING

Considering the fact that APPC do not have prior experience in implementing/managing various initiatives, training is required to develop a community who would be fluent in using the environment. Vendor provided training courses could be utilized for this purpose.

ROLES & RESPONSIBILITY

ROLE	PERSON	RESPONSIBILITY	INVOLVEMENT
Storage Engineering	Sampath Kumar	• Design	
Storage Engineering	Suresh Kumar	• Design	
Storage Engineering	Fibish Madathil	• Review	
Storage Engineering	Geok-Kwee, Tee	• Approval	
Wintel Engineering	Bay, Jeffrey	• Design	Design of Login solution for management server
WISE Engineering	Sood, Amit	• Review	Review from Security Engineering
Storage Integration	Vasudevan, Shaji	• Peer Review	
Storage Operations	Vathsavai, Bhaskara	• Peer Review	
Wintel Integration	Reddy, Venugopal	• Review	

TECHNICAL DESIGN**CURRENT ENVIRONMENT & PROJECT BACKGROUND**

The Global Distributed Storage Engineering has proposed the SAN secure Build configuration (in 2005). APPC's existing SAN configuration was built before proposal of these global guidelines. APPC Storage Operations had raised the CAP # 0854/0855-MCCA, in July 2005 to address the known issues in the SAN infrastructure. The Storage Engineering and Operations teams have since been working in understanding how to implement and customize the solution for APPC setup.

The potential risk were cited with respect to security and monitoring of the APPC SAN environment and Business Issues (BI) were reported during the August 2005 APPC mid-range/SAN audit.

APPC Storage Operations have initiated this project with the objective of formalizing the CAP implementation / gap closure exercise.

CONTINUITY OF BUSINESS (COB)

Necessary COB requirements have been taken into account while designing the infrastructure. Integration and operations personnel have agreed the same.

INFORMATION SECURITY

The initiatives have been designed based on global guidelines wherever applicable. However the design has also been reviewed by the BISO for compliance with Citigroup information security standards.

COMPLIANCE TO CITIGROUP STANDARDS (PRODUCT RCSA)

This is an initial deployment in APPC. Any product RCSA would be prepared and carried out later.

DESIGN CHECKLIST

Requirements to be covered as per the CAP was studied

The growth rate was determined for various initiatives

The minimum capacities, maximum capacity, end of support (sales, hardware and software) of different sub-systems were scrutinized.

The requirements to comply as per global guidelines were analysed.

PROPOSED DESIGN

Implementation, setup and configuration of the following modules are required in the APPC SAN environment in order to address the reported BI:

1. Log consolidation for Storage subsystems using eTrust audit
2. SAN change and monitoring tool (SANSscreen implementation)
3. Security enhancement in SAN fabric via implementation of SANTegrity
4. Solution Enabler implementation on SUN Solaris.
5. Setting up SOE remote management console for Clariion and Connectrix

DESIGN DOCUMENT



This project aims to provide recommendations, solution architecture for APPC Integration and Operations groups to successfully implement SAN Secure Build modules with the objective of addressing audit findings / BI reported in CAP #0847-MCCA. Following sections explain in detail, proposed solutions for the above-mentioned initiatives.

1. Log consolidation using eTrust Audit:

SCOPE

The scope of this module is to consolidate and review logs generated in the storage infrastructure like EMC, HDS etc. It is a global recommendation to use eTrust audit to consolidate all the storage logs. Logs to be consolidated are generated by applications like SymmRemote, Symmwin, Navisphere Manager, Connectrix manager and HDS storage Navigator. This project will ensure the setup of all in-scope applications with reference to Citigroup standard.

Following logs are in the scope of consolidation using eTrust Audit:

SymmRemote Log

Records date and time of when vendor gets connected / disconnected.

SymmWin Log

User activity logs on the service processor and changes to the Symmetrix array by the vendor

Clariion Log

Changes to Clariion arrays by system administrator or vendor through Navisphere application

HDS Log

Configuration changes to HDS arrays and user logins.

Connectrix Log

Logs of successful and unsuccessful attempts to access the Connectrix SVP remotely.

INSTALLATION PREREQUISITES

- eTrust Audit Client software (eac11510)
- EMC Log Pull program
- Message Parsing Files
- eTrust Audit Policy Manager Server Hostname and IP Address
- eTrust Audit Collector Server Hostname and IP Address
- Disk space
- Network connectivity
- Firewall ports (see Appendix)
- License

SymmRemote logs are collected in each service processor and events are automatically sent by eTrust to the collector server. Contact EMC to get the EMC log Pull program (swlfg.exe) which consolidates the symmwin logs into single location in the Service processor from where it can be pushed to collected server

The copy of the message-parsing file for each product is found in the eTrust Audit Storage monitor document (http://gdse.ny.smb.com/GDSE_docs/GDSE-05023-SG.pdf). Message Parsing files for each storage array can be created by cut/paste from the same document.

Contact platform team to get the fully qualified domain name of the policy manager server and collector server.

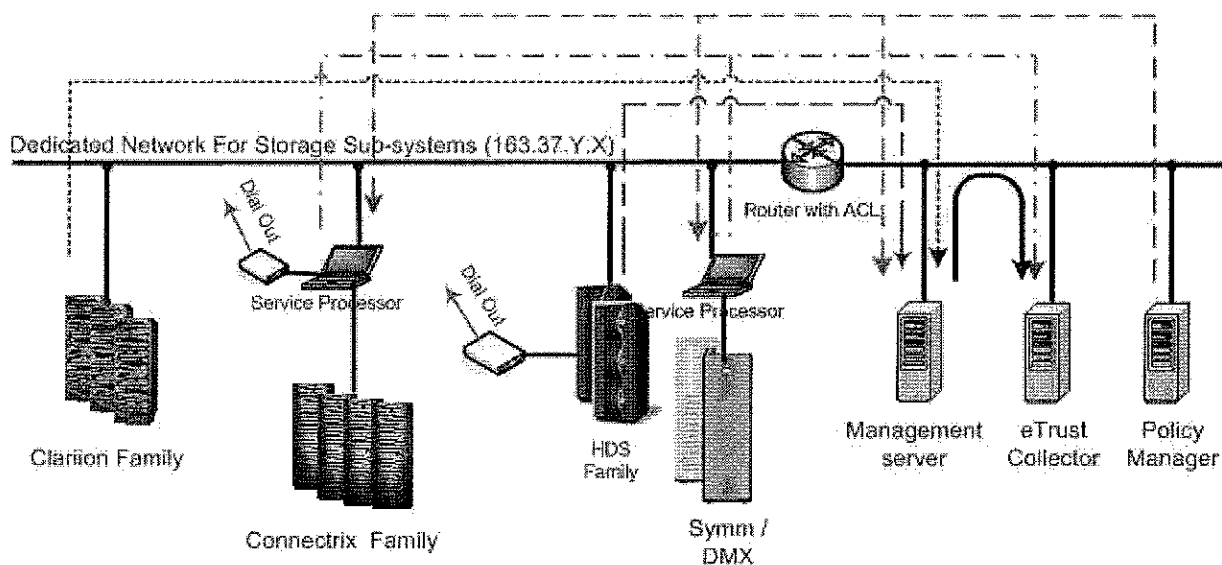
By considering the current storage infrastructure 72GB of storage space is required to collect logs in the collector server.

The eTrust Audit Client (Storage SP, HDS Management server, Connectrix SP or Navisphere Mgr) will need to have network connectivity and the ability to connect to the eTrust Infrastructure.

eTrust Audit client license (100 nos) should be purchased / informed to the Global ELA team as the global license has already exceeded.

SOLUTION DESIGN

The following diagram illustrates the eTrust Audit infrastructure from storage sub-systems:

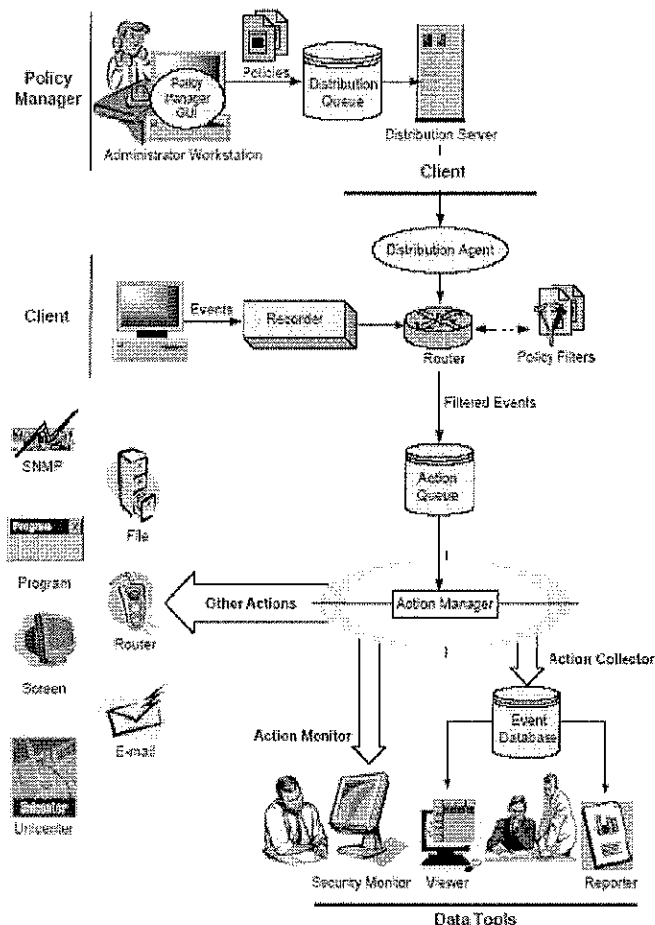


Legend

- > Automatic Log pull using NaviCLI
- > Policy Propagation from Policy Manager
- > Automatic Log push from Audit Clients to Collector
- > Manual Log Collection using Storage navigator
- > Automatic Log push to Collector Server

INSTALLATION OF eTRUST AUDIT CLIENT

The eTrust Audit client will be installed on the management servers and on every Symmetrix, DMX, and Connectrix service processors. These clients will be configured to pass events back to the eTrust Collector database for review. Only EMC authorized personnel are allowed to install and configure the client software and EMC Log pull software in a service processor. Detailed installation steps can be followed from section 8.1.1 of the eTrust configuration and solutions guide mentioned in Appendix A.

OVERVIEW OF eTRUST AUDIT ARCHITECTURE

An administrator uses the Policy Manager to create, activate, and distribute policies that are stored in the policy distribution queue and routed to Distribution Agents on clients. As events occur on clients, the Recorder harvests them and sends them to the Router for processing. Using the policies and filters created by the administrator, the Router stores events in the action queue for processing by the Action Manager.

The Action Manager, based on the policies specified, could send events to the Collector database where an administrator can use the Viewer to display events or use the Reporter to generate reports for later analysis.

2. Tracking SAN Changes using SANScreen

SANScreen from Onaro, is a SAN tool for monitoring and managing change control functions in SAN. It is based on the concept of logical access paths from Host to the Storage and monitors changes that affect the access path in the SAN.

The scope of this module is to track authorized /unauthorized changes in the storage infrastructure. SANScreen would also be used to alert about these changes, consequent violations (if any, based on pre-authorized parameters) and various vulnerabilities due the changes.

SANScreen also helps to analyze the impact of future changes by way of planning and validation in the existing environment. SANscreen is a non-intrusive tool and does not perform active configuration and management of SAN components. It is not intended for element management functions including component-level alerting and performance. It is also not intended for logging user activity in the SAN and detailed reporting functions.

Following are the currently supported environments by SANScreen:

- EMC Symmetrix / DMX and Clariion arrays
- HDS storage arrays
- McData and Brocade switches
- Switch-Host connectivity (Data is not collected directly from hosts)

SCOPE

Following are responsibilities in-scope using SANScreen:

- SAN-attached devices identification (and inventory)
- Available paths identification
- Creating policies and authorizing paths
- SAN-change identification (LUN masking, zoning, paths)
- Policy-based path violations identification
- Policy-based path vulnerabilities identification
- Planning SAN (path) changes

INSTALLATION PREREQUISITES

SANScreen Package (sans2960)

SANscreen server

Remote Acquisition Unit (RAU)

SANscreen client

Solution Enabler windows package (ewse6010)

Network connectivity to SE solaris server, Clariion domain, Hitachi DM and Connectrix SVP.

Symapi license on SE solaris server

Hicommand Device Manager license

Firewall ports (Please refer Appendix A)

License key

SANscreen server is the processing engine of SANscreen application and comprises of the database and a Local Acquisition Unit.

RAU (Remote Acquisition Unit) can also be installed on a dedicated server for large environments. SANscreen utilizes an https encrypted channel to send SAN change information to the server.

SANScreen server / Remote Acquisition Unit minimum Hardware requirements

Windows 2003 server

2 x 2.8 GHz CPU or better

4 GB RAM

Minimum 72 GB Mirrored RAID disk (SAN or Internal)

Dual 100Mbps NIC

Backup client (Standard backup software e.g. netbackup)

SANscreen client

SANscreen client can be run on any Windows 2000 Professional desktop. Its minimum requirements are:

1 X 1.5GHz CPU or better

512MB RAM

Java Runtime Environment (JRE) v1.4.2

Launched from user desktop via SANscreen web launch.

License Key

A valid license key is required to configure SANSCREEN. It is configured from the License Manager interface accessible from SANscreen's administrative web interface. There is a global license available for this product, which can be obtained from GDSE.

APPLICATION PREREQUISITES

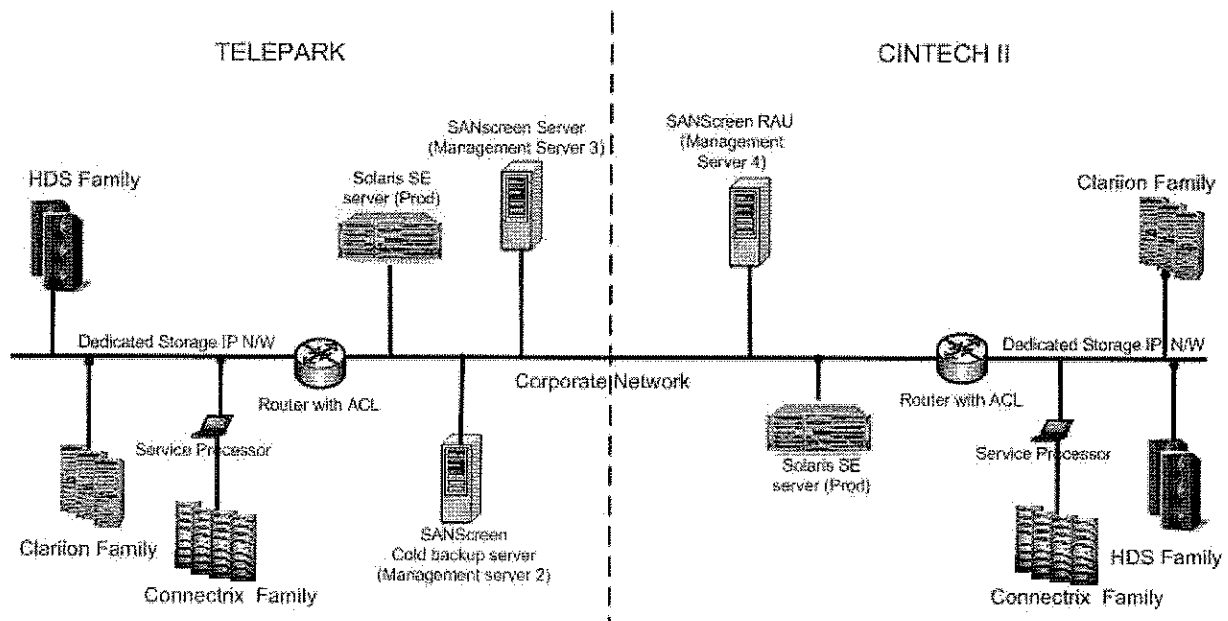
Application Component	Prerequisites	Notes
Sanscreen server		
Acquisition unit	Sanscreen Server	
Symmetrix Datasource	1.SYMAPI client on AU server 2.SYMAPI server connectivity 3.IP address of SE server	1. netcnfg and nethost on SYMAPI/SE server have be configured to enable access to SANscreen AU server 2. SYMAPI BASE/SERVER and devmasking licenses should be enabled on the symapi server.
Clariion Datasource	1. IP address of Navisphere 2. Read-only userID for SANscreen on Navisphere.	
McData Datasource	1. EFCM server IP address 2. View rights userID for SANscreen on EFCM.	
HDS Datasource	1. IP address of HiCommand DM 2. Guest userID on Device Manager	

Desktop GUI	Java Runtime Environment (JRE)	
-------------	--------------------------------	--

SANSCREEN INSTALLATION , BASIC CONFIGURATION, USER ROLES, BACKUP & RESTORE

Please see the given document link for detailed step by step info
http://gdse.ny.ssmb.com/GDSE_docs/GDSE-05053-SG.pdf

SANSCREEN ARCHITECTURE



3. Security Enhancement of SAN Fabric using SANtegrity

SCOPE

The scope of this project is to implement the SANtegrity functionalities for McData switches in the APPC datacenter.

Following are the SANtegrity features will be in scope of this module:

- Implement Port binding on all switch ports including empty ports (License not required)
- Implement fabric binding with insistent domain id (SANtegrity license is required)

OUT OF SCOPE

SANtegrity Features	Remarks
Switch Binding	Not recommended by citigroup
Enterprise Fabric mode	Not recommended by citigroup
RSCN Zone isolation	Supported only from E/OS 7.0x and CM 8.7.1 versions
IP Port Hardening	Supported only from E/OS 7.0x and CM 8.7.1 versions
RBAC in SANav	Supported only from E/OS 7.0x and CM 8.7.1 versions
Logging	Supported only from E/OS 7.0x and CM 8.7.1 versions
Eport Fencing	Supported only from E/OS 7.0x and CM 8.7.1 versions

In future, after the certification of above said versions, the respective SanTegrity features would be configured to enhance SAN security.

REQUIREMENTS

Requirements	
Switch Models	DS-16M2, DS-24M2, DS-32M2
Director Models	ED-64M, ED-140M
E/OS Versions	06.01.00
CM Versions	7.01.00, 7.02.00
License	SANtegrity I fabric binding license (Global License)

LICENSE ACTIVATION PROCEDURE

To enable certain SANtegrity features (Fabric Bindings), a license string must be entered. To enter 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 switches will IPL and have a momentary loss of LAN connectivity¹⁴. Select the Yes button on the warning screen.

At this point the switch may quit responding (Ethernet only) for a few seconds and the status may show link down but it will come back to operational.

Once the license is entered, the switch will have SANtegrity binding license enabled so that fabric bindings could be configured.

CONFIGURING SANTEGRITY

Both Port and Fabric Bindings can be done without the need for downtime. Port Bindings can be configured and cleared without any ports going on or offline as long as cables are not moved while the bindings are taking place. Fabric Bindings can be configured and un-configured without fabric rebuilds as long as all switches are added in the membership list at the start of the process. Plans should be made however not to do zoning and LUN Assignment during the time that both Fabric and Port Bindings are being configured. For the detailed procedure description of port binding and fabric binding, please see Section 14 of the McData Management solutions guide mentioned in Appendix A.

BACK-OUT PLAN

Backup out of both Port and Fabric Bindings can be done while the fabric stays online. To back out of Port Bindings, and administrator needs to do the following:

- Call up the Configure Ports screen for the switch in question from the hardware view of Connectrix Manager.
- Right click in the Port Binding column and select Unbind all WWN from the drop down menu.
- Right click in the Port Binding column and select Clear all Bound WWN from the drop down menu.
- Hit the Activate button at the bottom of the screen.

To backout of Fabric Bindings, the Administrator would need to do the following:

- Go to the fabric view of Connectrix Manager and highlight or select the fabric in question.
- Call up the Fabrics menu and then select Fabric Bindings from the pull down menu.
- Uncheck the Enable Fabric Binding checkbox.
- Go through the remainder of the screen until the activations can occur to disable fabric bindings and hit the Activate button.
- Insistent Domain ID will remain active on all switches that were bound.

4. Solutions Enabler Migration to Solaris

SCOPE

The scope of this module is to migrate, only the LUN masking from the existing HP-UX Solution Enabler server to a Solaris Server.

REQUIREMENTS

The host should be connected to SAN to which the Symmetrix storage arrays that are to be managed are connected. At least two gatekeeper devices from every Symmetrix/DMX array should be zoned and masked to this host. Powerbroker is required to restrict and log access of all actions performed on the SE solaris server.

HARDWARE/SOFTWARE REQUIREMENTS:

Solaris SOE 8 Build Tier 2 Server (Five Nos including one UAT server)

2CPU/ 4GB RAM / 72GB DISK from SAN

DUAL NIC

3 - 4 Emulex HBA Cards (Depending on the connectivity to Symm/DMX arrays from each SE)

EMC Solution Enabler 5.5 SPAC package emcsolena5.5.0_A2 or latest certified version.

Licenses – collect from EMC

(BASE, DEV- MASKING, CMODE, TIMEFINDER)

At least two gatekeepers and VCMDB device from every symm array

PowerBroker – Reference http://gdse.ny.smb.com/GDSE_docs/Proposed/GDSE-05006-S.pdf

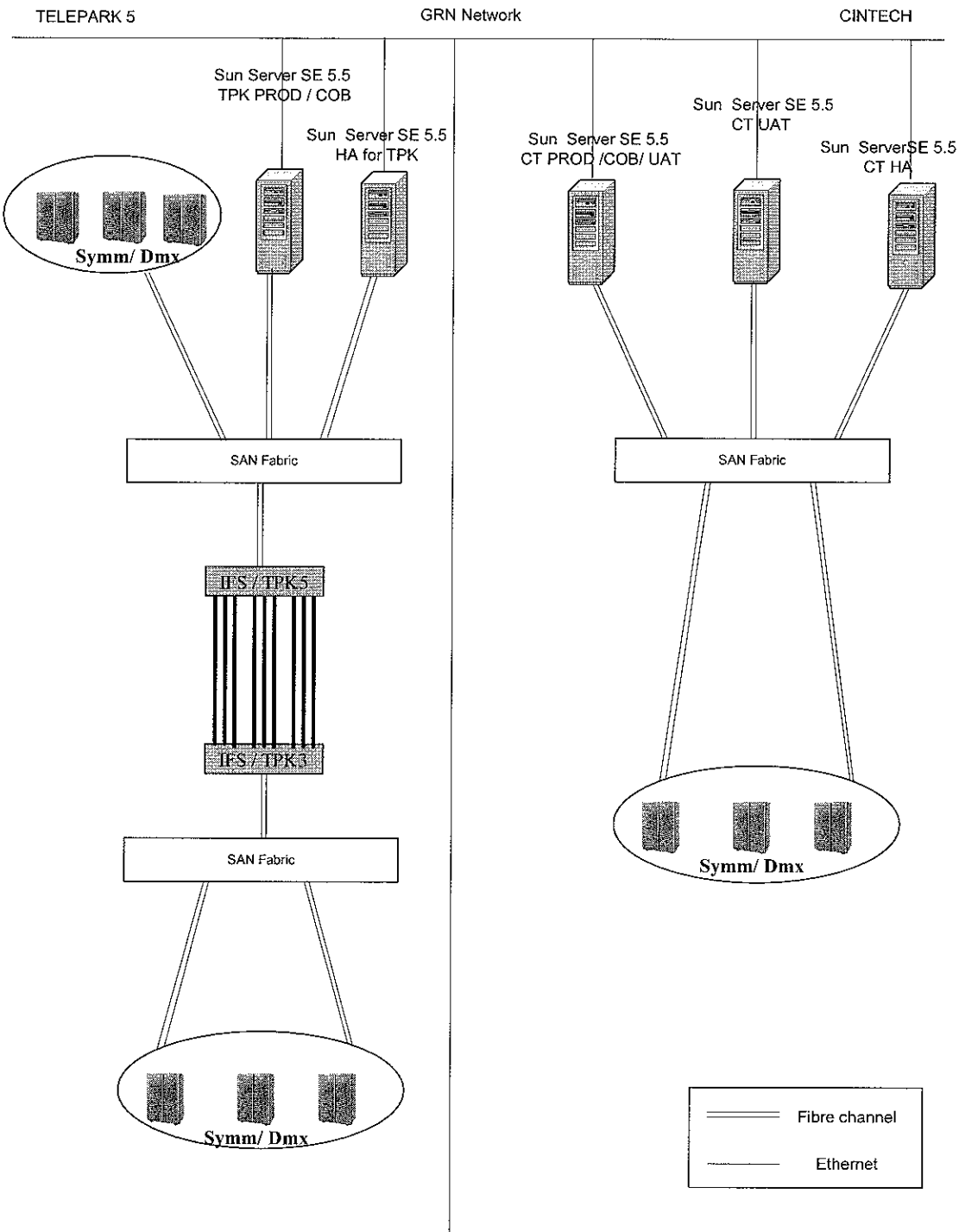
SOLARIS 8 CONFIGURATION MATRIX:

SOE Patch Level	8
HBA	LP9002
HBA Driver	6.02e
HBA Firmware	3.92a3

There are five servers proposed for the SE migration, in which two servers on each side for redundancy and the fifth server on CINTech for the UAT boxes. The server roles are self explanatory from the proposed configuration diagram.

Note : In future, to support incremental clone functionality, Solution Enabler software has to be upgraded to 6.x on HP-UX BCV management host. This version would not be certified on HP-UX by GDSE as the future Solution Enabler versions would be certified only on solaris. As a standard, Solution Enabler versions running on Solaris and HP-UX should be the same.

DESIGN DOCUMENT
PROPOSED CONFIGURATION



INSTALLATION PROCEDURE AND USER PRIVILEGES

To install Solutions Enabler 5.5 on a SOE Solaris 8 host, install the Solaris package emcsolena5.5.0_A2 from the GDS distribution server. Accept default options. This will completely install the SE 5.5 application on the host under /export/opt/emc.

The following /etc/system parameters must be set:

```
set semsys:seminfo_semmni=600
set semsys:seminfo_semmns=600
set semsys:seminfo_semtime=600
set semsys:seminfo_semmnu=600
set shmsys:shminfo_shmmax=1048576
set shmsys:shminfo_shmmni=600
```

The host should be rebooted after setting these parameters.

Only authorized storage operators should be configured to log on to the host. Each operator should be assigned their unique user ID, such as SOE ID, to logon to the host. The user IDs so assigned should be unprivileged (non-root). Each storage operator's account should be profiled with the following: The PATH environment variable should include the location of the SE binaries at /usr/symcli/bin.

All the symcli binaries involving change functions should be accessible only by root. Each storage operator will be granted access to execute all symcli commands necessary for their functions. This access will be controlled by the Powerbroker, which restrict and log access of all actions performed on the SE server.

MIGRATION PROCESS

ON EXISTING SE SERVER

Run symcfg discover to make sure information in the symapi database is up to date.

Backing up VCMDB

It is recommended to backup vcmdb in case of corruption caused by other factors.

```
# symmaskdb -sid SymmID -file </var/HPSE/BackupFileName> backup
```

Backing up Symapi

Create copies of the host database and config directories (/var/symapi/db and /var/symapi/config)

(For example) # cp /var/symapi/config/symapi_db.bin /var/HPSE

Backup customized scripts

Copy all customized scripts used for lun-masking to /var/HPSE

Exporting the device groups

If any BCV groups are not application oriented, with the concurrence of platform support team it can be moved to new SE solaris server. Create sub-directories using the Symmetrix serial id to separate device groups for each symm.

```
# mkdir /var/HPSE/<sid>
# symdg -f /var/HPSE/<sid>/BCV1.txt export <BCV grp name>
```

ON NEW SE SERVER

Install solaris 8 SOE and latest certified SE 5.5
Zone and Mask new SE server to Symmetrix(s) FA ports
Apply the required SE licenses using symlmf command

Build the SYMAPI database

Run symcfg discover command to build your configuration (SYMAPI) database. This needs to be done once after installation, and after any changes are made to your Symmetrix configuration.

Add VCMDB device to the SE server

```
symmask -sid xxxx -wwn <xxxxxx> -dir ## -p # add dev 0000
```

Importing device groups

Copy all backed up/exported files to new Server (/var/HPSE)

```
# symdg -f /var/tmp/<sid>/BCV1.txt import <BCV Grp name>
```

Adding standard device <xxx> as DEV001...

Associating remote BCV <xxx> as BCV001...

Verifying the configuration

Symdg list, symrdf query, symmir query and perform symmaskdb functions

Perform symcfg discover to ensure that the Symmetrix(s) remain visible to the SE server.

Backup VCMDB and Symapi database

Schedule routine backup of symmaskdb and symapi database using existing backup scripts

BACK-OUT PLAN

The lun masking licenses on existing HP-UX SE servers will be removed only one week after the successful migration of SE to new Solaris server. If you face any problem during the migration you always can fall back to existing HP-UX server to continue the normal operation.

5. Management server for SAN Management

INTRODUCTION

With the ever-increasing growth in SAN infrastructure, it is currently very hard to track and log activities carried out in it and there are no measures in place to prohibit a dial in and have control on the vendor connectivity for storage sub-system administration. The SAN secure initiative addresses this, by providing the Vendor Remote Access through WWDS and, by having a server dedicated to do SAN management.

SCOPE

The scope of a management server is to provide a central entry point for storage admin personnel to get connected to do SAN management. The management server is setup to manage sub-systems like Clariion, HDS & Connectrix switches. This server would also log activities as per the eTrust Audit initiative and send for review. Also, the server would host applications like SANScreen to monitor and alert changes happening in the SAN. It is planned to expand the administrative scope of this server by including components like CentricStor, Decru etc in the future.

DEPENDENCIES

The Log consolidation portion is dependant upon timely setup and availability of eTrust Audit servers.

HDS change monitoring using SANScreen is dependant on upgrade of all HDS sub-systems to the certified micro-code level and procurement of license for HiCommand Device Manager.

ARCHITECTURE

The architecture consists of management servers at each floor of the data centre. The connectivity and software used in them differ as required. All the servers would have minimum of 2 NICs. The servers would be connected to the GRN. The storage sub-systems like HDS, Clariion, Connectrix, Symmetrix, DMX etc are connected to the dedicated storage IP network isolated through a router with ACL. Vendors, who need to access systems in this network, would come through WWDS. The storage operations personnel would access them from GRN normally. Necessary firewall ports have to be opened to access different software applications by the management servers. Please refer to Appendix A on the necessary port opening requirements.

CLARIION MANAGEMENT:

The Clariion storage sub-systems are managed by the navisphere manager application. All the clariion SPs are connected to the dedicated storage IP network. The clarion SPs could be accessed externally only through the management server. The navisphere manager application runs in the management server and it will be used to dial out alerts to EMC. The Navisphere Web application is configured to run on the Clariion SPs. The support personnel would have to login to the management server and do the administration typically by launching the management server's web browser, which will access the navisphere application. For further references about clarion management, please refer to the product best practices guide at mentioned in Appendix A.

The management servers dedicated for Clariion alert notification, would have a modem connected to them. These servers would host the event-monitoring module of the navisphere application for the above purpose. For any alerts generated within the Clariion domain, the management server would call home and notify with necessary data. Please refer Appendix A for the communications about the necessary approval obtained for the dial-out to happen in these servers.

For the log consolidation purpose, log pull programs are configured to pull activity logs from all Clariion SPs using NaviCLI. The log pull programs would have to run once every day through the task scheduler or any job scheduling software. The eTrust Audit Client would be configured to send the alert events to the central consolidation infrastructure based on the collected information. For further information, please refer Appendix A for the Solution Guide and the storage engineering solution document for log consolidation using eTrust.

CONNECTRIX MANAGEMENT:

The Connectrix sub-systems are managed by the Connectrix manager application. The Connectrix service processors are connected to their respective dedicated storage network. The Connectrix manager clients running in the management console would access the Connectrix manager server process running in each Connectrix service processor. The management personnel would have to launch the Connectrix manager client after login to the management server, in order to do the administration.

For further explanation about Connectrix management, please refer to the McData Solution Guide mentioned in Appendix A.

HDS MANAGEMENT:

The administration of Hitachi storage sub-systems could be currently done using two applications, namely Device Manager and Storage Navigator. The HDS service processors are connected to their respective dedicated storage network. Individual storage navigator server applications run in each of the HDS service processors. These server applications could be accessed from web browsers.

The Hitachi HiCommand Device manager is a centralised approach to do the administration of all Hitachi sub-systems from a single window. The Device manager application runs in the management server and would be configured to access all the storage sub-systems with administrative privilege. Device manager application could be accessed through the web browser. For security reasons, the Device Manager web service could be configured to access only from the local host.

The support personnel would have to login to the management server and do the administration typically by launching the management server's web browser, which will access either the storage navigator server or the device manager, whichever is required. However, Global directive is to use HiCommand Device manager for managing the HDS sub-systems due to its seamless integration with eTrust Log consolidation and the SANScreen initiatives.

For further explanation about HDS management, please refer to the HDS Solution Guide mentioned in Appendix A.

SANSCREEN APPLICATION:

In addition to the administration of storage sub-systems, the management server would also host applications to monitor and track the changes happening in the SAN. One such initiative is the SANScreen application, which would communicate with various SAN administration tools like the Navisphere manager, Connectrix Managers, Symmetrix/DMX solution enabler hosts and Hitachi Device Manager and record changes done in each of the respective sub-systems. Minimal reporting functionality has been provided in this application to view the authorized / unauthorised changes. This application communicates only through the IP network and hence no fabric connectivity is required. Sufficient hardware requirements have been factored in sizing the servers hosting the SANScreen application. Please refer Appendix A for communications emphasizing about required hardware for running this application.

For larger environments, it is recommended to split the functionality of monitoring the infrastructure using remote acquisition units (RAU). These RAU, would preferably run dedicated data sources for a particular type of a storage sub-system (e.g. Clariion or Connectrix only). These sources would then report to the central monitoring server for consolidation.

Please refer to the dedicated section in this document for further information about SANScreen,.

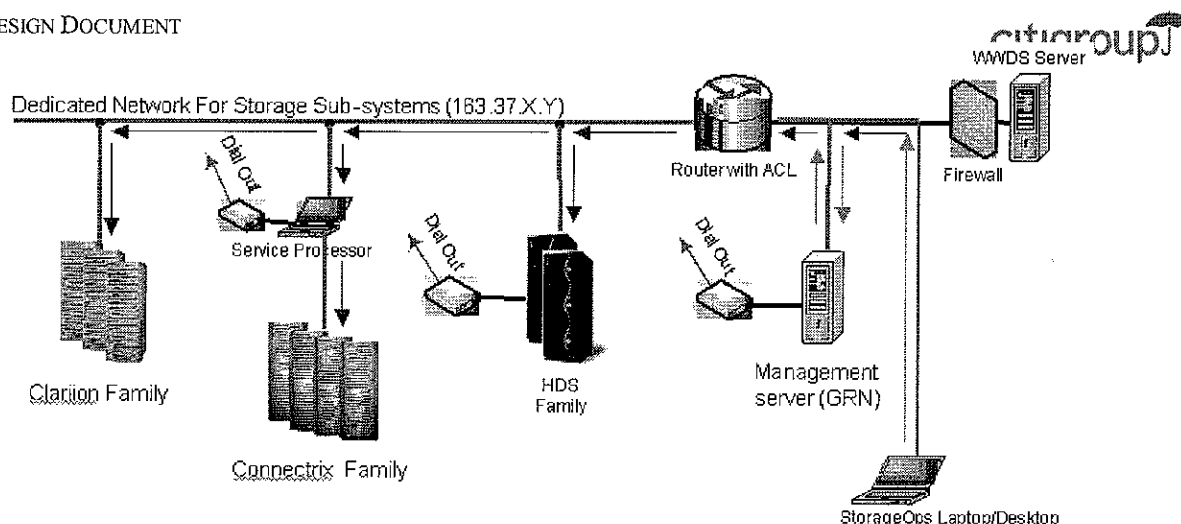
LOGIN SOLUTION FOR MANAGEMENT SERVERS

The management servers would act as dedicated central points for storage administration and only storage operations personnel would access them. Following sections explain the login procedure for the operations personnel to access the management server.

LOGIN WORK FLOW

In the following diagram, workflow of management servers access is illustrated with blue arrows. More detailed diagrams can be found in later sections.

- Storage Operations personnel connects to the management servers via his dedicated SOE workstation/laptop from the Citigroup network
- He then logs in to a Terminal Server session locked down by the soec1130 wrap, and will have access, only to the required storage management applications and folders. The storage management applications have to be Terminal Server 2003 aware.
- The storage management application will then administer the various subsystems in the storage network by going through the Router with ACL.



HARDWARE REQUIREMENTS FOR PROPOSED SERVERS

The management servers will be deployed with the following configurations:

SI No.	Location	Env	Specification	Software Required	Purpose
1	TPK3	Prod	2 CPU, 4 GB, 2 HBA, 2 NIC	CNX Manager Client, Etrust Audit Client, JRE**	HDS Management, CNX Management and Log Consolidation
2	TPK5	Prod	2 CPU, 4 GB, 2 HBA, 2 NIC	Navisphere Manager, CNX Manager Client, Etrust Audit Client, SANScreen RAU, JRE**	HDS Management, CNX Management, Clariion management, SanScreen and Log Consolidation
3	TPK5	Prod	4 CPU, 8 GB, 2 HBA, 3 NIC	Navisphere Manager, CNX Manager Client, Etrust Audit Client, Sansscreen Server, JRE**	HDS Management, CNX Management, Clariion management, SanScreen and Log Consolidation
4	CT2	Prod	4 CPU, 8 GB, 2 HBA, 3 NIC	Navisphere Manager, CNX Manager Client, Etrust Audit Client, Sansscreen Server, JRE**	HDS Management, CNX Management, Clariion management, SANScreen and Log Consolidation
5	CT2	Prod	2 CPU, 4 GB, 2 HBA, 2 NIC	Navisphere Manager, CNX Manager Client, Etrust Audit Client, SANScreen RAU, JRE**	HDS Management, CNX Management, Clariion management and Log Consolidation
6	CT2	UAT	2 CPU, 4 GB, 2 HBA, 3 NIC	Navisphere Manager, CNX Manager Client, Etrust Audit Client, Sansscreen Server, JRE**	HDS Management, CNX Management, Clariion management, SANscreen and Log Consolidation

- 2 CPU 4 GB servers will be DL380 G4s:

<http://www.citigroup.net/tie/de/wintel/standards/hardware/servers/Compaq/serverspecs/dl380g4-term.htm>

- 4 CPU 8 GB servers will be DL580 G3s:

** The required version of JRE will be 1.4.2

SERVER OS BUILD DOCUMENTS

- The management servers will be Wintel servers running Windows 2003 with Terminal Services role installed.
- All wintel management servers are to be joined to the APAC domain.
- Refer to the following section for Client Access License information.
- Refer to: <https://integration.ti.citigroup.net/newww/project.asp?PID=94&CID=5> under PSE VTM Certified Wintel Builds - Windows 2003, for required SOE and VTM wraps.

CLIENT ACCESS LICENSES

The licensing for 10 “per user” Client Access Licenses will be purchased for each management server running terminal services, which will number 60 for the total number of CALs purchased. Each terminal server will also be installed with the terminal server licensing services, which will manage the CALs on the respective terminal server. The existing enterprise licensing servers will not be used.

ASSUMPTIONS AND RISKS

Assumptions

- There will not be more than 10 concurrent terminal service client hardware devices connecting to each management server.
- This design might be revised at a later date during a post-implementation review to align with TI's server consolidation initiative.

Risks

- This project is bound by a tight timeline, which needs to be implemented by End June 2006 for UAT and End August 2006 for production.

SERVER ROLES

The management servers would act as dedicated central points for storage administration and only storage operations personnel would access them.

Please refer to following section for the proposed management architecture. Also, please go through reference documents in Appendix A for details about the configuration of each of the components.

One management server (Management server 1) is proposed to be in TPK3, as personnel working there would take direct access of the server at any time and complete their activity.

Management server 3 at TPK5 will act as Call Home server for Clariion family in Telepark. This server will also act as the SANScreen master monitoring server, Log consolidation server and Client for Connectrix & Clariion.

Management server 2 at TPK5 will basically act as a Cold Backup to the SANScreen master in TPK. Importing SANScreen configuration database from the master and starting the service could continue the SAN change monitoring. This server will also share client sessions initiated for TPK5.

Management server 4 at CT2 acts as the SANScreen remote acquisition unit for management server 3. This server will also act as Call home server for Clariion family in CT2.

Management server 5 at CT2 could act as a backup for management server 4. This server will also share client sessions initiated for CT2.

The UAT management server at CT2 will primarily be used as a staging server for software upgrades and configuration testing before porting them to the production management servers.

CONTINGENCY REQUIREMENTS

- There would be a pair of management servers for redundancy and load sharing each at TPK5 and CT2.
- Management server 2 at TPK5 is the redundant server (not HA) for management server 3 in case of a SANScreen application failure in management server 3.
- It should be noted that in case of Management servers 3 or 4 being down (scheduled / unscheduled), call home notification for the respective clarion sub-systems cannot happen.
- All management servers will be backed up as per APPC production standards for files.

INFORMATION SECURITY

- All the management servers will be SOE built and adhere to the approved Citigroup Security Standards.
- Terminal server sessions will be locked down by the soec1130 wrap. This wrap enables various feature lockdowns and the same settings will apply to both remote terminal sessions and physical console logins.
- Ports are required to be opened through the router ACLs between the storage network and the GRN. This is to facilitate communication between storage administration applications residing on the management servers and the storage subsystems in the protected network.

ACCESS CONTROL MATRICES

The following tables reflect the additional NTFS permissions and rights to be applied for access control on the specific application folders/executables on the management servers. Permissions for other standard folders are already accounted for by the SOE build and will not be included.

WINDOWS 2003

Group	User Rights	Justification
StorageOps Group	Normal authenticated user rights	This ID Group is for Citigroup Storage Operations personnel

User Name	Local Server Group	User Rights	Justification	Servers
APAC\{storageops SOEIDs}	StorageOps Group	- Logon locally	Storage subsystem	{TPK3 Management Server} {TPK5 Management Server 1}

			administration	{TPK5 Management Server 2} {CT2 Management Server 1} {CT2 Management Server 2} {CT2 UAT Server}
--	--	--	----------------	--

{ MANAGEMENT SERVER1 - TPK3 }

Drive C

Directory	User ID & Group	Permission
C:\PROGRAM FILES\EFCM (CNX MANAGER CLIENT APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
D:\STORAGE\LOGS D:\STORAGE\HDSLOGS (STORAGE APPLICATION LOG FILES)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Write/ Execute

Drive J

Directory	User ID & Group	Permission
J:\APPS_PUB\MSIE6050 (STANDARD SOE MICROSOFT INTERNET EXPLORER WRAP FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

{ MANAGEMENT SERVER 2 - TPK5 }

Drive C

Directory	User ID & Group	Permission
C:\PROGRAM FILES\EFCM (CNX MANAGER CLIENT APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
C:\PROGRAM FILES\SANSCREEN (SANSCREEN APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
D:\STORAGE\LOGS D:\STORAGE\HDSLOGS	Admin Group	Full Control
	Everyone	None

(STORAGE APPLICATION LOG FILES)	StorageOps

Drive J

Directory	User ID & Group	Permission
J:\APPS_PUB\MSIE6050 (STANDARD SOE MICROSOFT INTERNET EXPLORER WRAP FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

{ MANAGEMENT SERVER 3 – TPK5 }**Drive C**

Directory	User ID & Group	Permission
C:\PROGRAM FILES\EFCM (CNX MANAGER CLIENT APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
C:\PROGRAM FILES\SANSCREEN (SANSCREEN APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
D:\STORAGE\LOGS D:\STORAGE\HDSLOGS (STORAGE APPLICATION LOG FILES)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Write/ Execute

Drive J

Directory	User ID & Group	Permission
J:\APPS_PUB\MSIE6050 (STANDARD SOE MICROSOFT INTERNET EXPLORER WRAP FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

{ MANAGEMENT SERVER 4 – CT2 }**Drive C**

Directory	User ID & Group	Permission
-----------	-----------------	------------

DESIGN DOCUMENT

C:\PROGRAM FILES\EFCM
(CNX MANAGER CLIENT APPLICATION FOLDER)

Admin Group



Everyone

None

StorageOps

Read/Execute

Directory	User ID & Group	Permission
C:\PROGRAM FILES\SANSCREEN (SANSCREEN APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
D:\STORAGE\LOGS D:\STORAGE\HDSLOGS (STORAGE APPLICATION LOG FILES)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Write/ Execute

Drive J

Directory	User ID & Group	Permission
J:\APPS_PUB\MSIE6050 (STANDARD SOE MICROSOFT INTERNET EXPLORER WRAP FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

{ MANAGEMENT SERVER 5 – CT2 }

Drive C

Directory	User ID & Group	Permission
C:\PROGRAM FILES\EFCM (CNX MANAGER CLIENT APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
C:\PROGRAM FILES\SANSCREEN (SANSCREEN APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
D:\STORAGE\LOGS D:\STORAGE\HDSLOGS (STORAGE APPLICATION LOG FILES)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Write/ Execute

Drive J

Directory	User ID & Group	Permission
J:\APPS_PUB\MSIE6050 (STANDARD SOE MICROSOFT INTERNET EXPLORER WRAP FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

{MANAGEMENT SERVER 6 - CT2, UAT SERVER}

Drive C

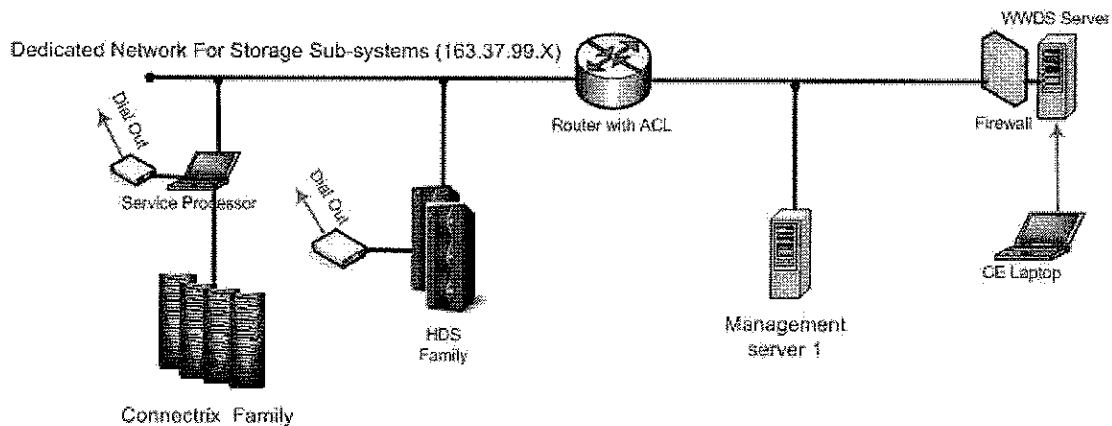
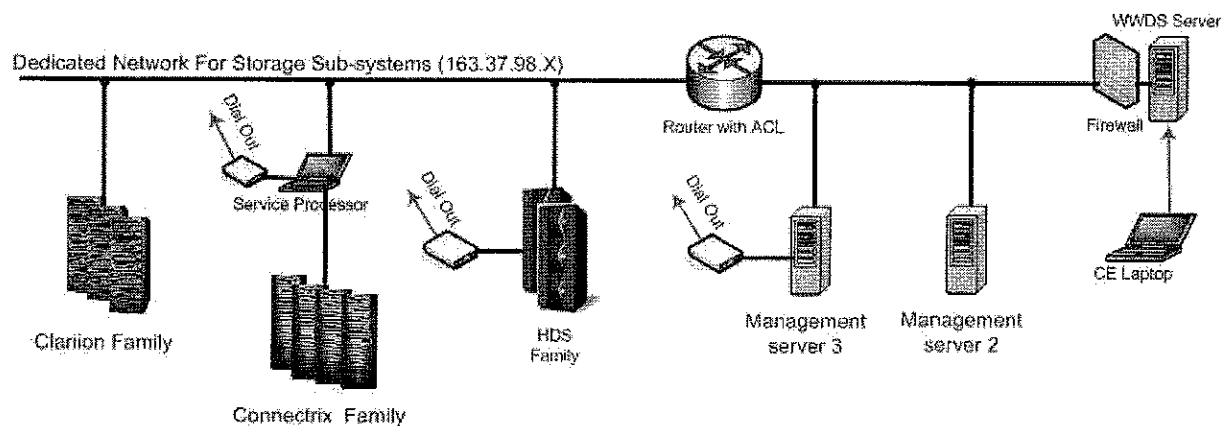
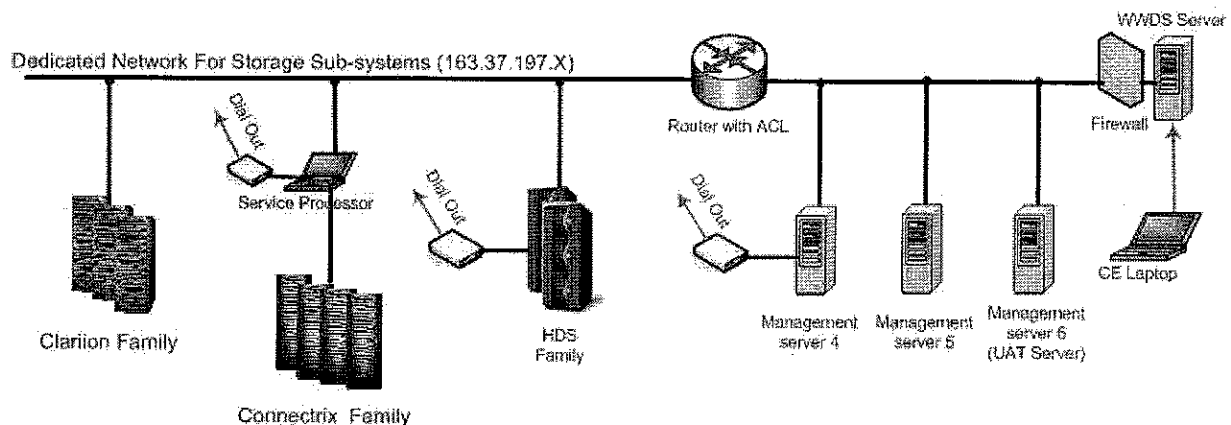
Directory	User ID & Group	Permission
C:\PROGRAM FILES\EFCM (CNX MANAGER CLIENT APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
C:\PROGRAM FILES\SANSCREEN (SANSCREEN APPLICATION FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

Directory	User ID & Group	Permission
D:\STORAGE\LOGS D:\STORAGE\HDSLOGS (STORAGE APPLICATION LOG FILES)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Write/ Execute

Drive J

Directory	User ID & Group	Permission
J:\APPS_PUB\MSIE6050 (STANDARD SOE MICROSOFT INTERNET EXPLORER WRAP FOLDER)	Admin Group	Full Control
	Everyone	None
	StorageOps	Read/Execute

PROPOSED INFRASTRUCTURE**Location : Tele Park 3rd Floor****Location : Tele Park 5th Floor****Location : Cintech II**

BUDGET

Summary of Anticipated Costs for Storage

Total Capital:	\$
Total One Time Expense:	\$
Total Annual Recurring Costs:	\$ 89, 827
Total Work Effort:	\$ 251, 935

Please see **APPENDIX C** for Bill of Materials & Resource costs

ITEMS	ACTION/TASKS	TEST PLAN/SCRIPTS	SIGN-OFF
Various initiatives have been tested, validated and accepted as a part of the POC conducted for this NSR.	POC has been done	Please refer the POC document	 POC Sign-off.pdf

APPENDIX A

- ETrust Configuration and Solutions Guide
http://gdse.ny.ssmb.com/GDSE_docs/GDSE-05023-SG.pdf
- HDS Management Solutions Guide
http://gdse.ny.ssmb.com/GDSE_docs/GDSE-05015-SG.pdf
- Clariion management Solutions Guide
http://gdse.ny.ssmb.com/GDSE_docs/GDSE-05010-SG.pdf
- Clariion management Best Practices Guide
http://gdse.ny.ssmb.com/GDSE_docs/GDSE-03011-B.pdf
- McData Management Solutions Guide
http://gdse.ny.ssmb.com/GDSE_docs/GDSE-04046-SG.pdf
- SANScreen Solutions Guide
http://gdse.ny.ssmb.com/GDSE_docs/GDSE-05053-SG.pdf
- Vendor Remote Access using WWDS Solution Document



EMC_Solution_7.doc

- Logon Solution for Management Server and related configuration information



RE (NSR 2005 1026)
SG-CTI SAN Secure E

- Communication about Hardware requirements for SANScreen application



RE Sanscreen - HW
and Sw details for ea

- Communication about the approval for using dial-out in the management servers



RE Resolved -
Connecting dial-out n

- Port opening requirements for different initiatives across the router with ACL.



"Port
Requirements_V3.xls"

- Clarion connectivity acceptance from global storage engineering.



RE CEP and
clarion.msg

- Approval from ISTG to use router with ACL.



RE Justification - RE
For your attention - R

Detailed Project Plan :



san_secure_build_v1
.5.2updated.mpp

APPENDIX C

L3 Estimates (Detailed Estimates)

Staff Expenses									
Item Category	Item Group	Details	Cost Center & Stream	Country	SOE ID	Unit Cost	Total Hours	FTE	Total Cost
Manpower	Manpower	Storage Engineering	8144 STORAGE ENGINEERING	Singapore		57.54	2500	17.86	143,850.00
Manpower	Manpower	Storage Integration	8017 STORAGE INTEGRATION	Singapore		22.98	2000	14.29	45,960.00
Manpower	Manpower	Storage Operations	8022 ENT STORAGE	Singapore		24.85	2500	17.86	62,125.00
Total									251,935.00
Citigroup Charges									
Item Category	Item Group	Item Details	Cost Center & Stream	Country	Env.	Install Date	Qty	Unit Cost	Total Cost
DASD	EMC (DMX/SYMMETRIX)	DASD for PRD SE.	8022 ENT STORAGE	Singapore	PROD	4/1/2006	544	66	35,904.00
DASD	EMC (DMX/SYMMETRIX)	DASD for Management Servers	8022 ENT STORAGE	Singapore	PROD	4/1/2006	432	66	28,512.00
DASD	EMC (DMX/SYMMETRIX)	DASD for UAT SE.	8022 ENT STORAGE	Singapore	UAT	4/1/2006	136	66	8,976.00
Tapes/Media	Tapes/Media	Tape infra unit cost based on DASD for UAT SE.	8022 ENT STORAGE	Singapore	UAT	4/1/2006	136	14.78	2,010.08
Tapes/Media	Tapes/Media	Backup unit cost based on DASD for Management Servers	8022 ENT STORAGE	Singapore	PROD	4/1/2006	432	14.78	6,384.96
Tapes/Media	Tapes/Media	Backup unit cost based on DASD for PRD SE Servers	8022 ENT STORAGE	Singapore	PROD	4/1/2006	544	14.78	8,040.32
Total									89,827.36