



Global Distributed Storage Engineering

Solutions Enabler 6.4 Certification

GDSE-07060-SG
Solutions Guide
Version 1.0

©Citigroup Inc. 2008, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

VERSION CONTROL

Version	Date	Author	Reviewed	Comments
<i>This is an update to the previous Solutions Guide for Solutions Enabler 6.3</i>				
0.1	Dec-12-2007	Quang Le	Guy Shimabuku, Chris Clayton, Ludwig Derodel, Parul Jain	SE 6.4 – Peer Review. Please see 10 Appendix C: Release Notes for changes since the last version of this document.
0.2	Dec-20-2007	Quang Le	Global Stakeholders	Release for Comments
1.0	Jan-25-2008	Quang Le	-	Release for Production

CONTENTS

VERSION CONTROL.....	2
CONTENTS.....	3
LEGAL NOTICE	5
CONTACT	5
LATEST VERSIONS.....	5
CONFIDENTIALITY	5
1 INTRODUCTION.....	6
1.1 APPLICABLE ENVIRONMENTS	6
1.2 RELEASE NOTES.....	6
2 CERTIFIED FEATURES OF SOLUTIONS ENABLER.....	7
2.1 SRDF/A FEATURES.....	7
2.1.1 Concurrent SRDF/A and SRDF/S from a single source.....	7
2.1.2 Support for multiple SRDF/A Groups	8
2.1.3 Availability	8
2.1.4 SRDF/A Write Performance	8
2.1.5 Dynamic Pair Operations for SRDF/A.....	8
2.1.6 SRDF/A Statistics Enhancements	8
2.2 2-SITE SRDF/MSD.....	8
2.2.1 Multi Session Consistency (MSD) Daemon Support.....	8
2.2.2 GNS Enhancements	9
2.2.3 SRDF/MSD	9
2.3 TIMEFINDER/CLONE.....	9
3 INSTALLATION PREPARATION	11
3.1 HOST.....	11
3.2 SYMMETRIX SECURITY	11
3.2.1 SYMACL Permissions.....	11
3.2.2 VCMDB Access	13
3.3 LICENSING.....	13
4 INSTALLATION	15
4.1 INSTALLING SE 6.4 ON SOLARIS 8 AND 10.....	15
4.1.1 System Requirements	15
4.1.2 Pre-Installation Procedure.....	15
4.1.3 Package Installation.....	15
4.1.4 Post-Installation Configuration.....	18
4.2 BACKING OUT OF AN UPGRADE.....	19
4.3 INSTALLING SE 6.4 ON HP-UX 11.11.....	19
<i>HP-UX is not the standard management platform for the Symmetrix within Citi. This package for HP-UX servers is to provide special applications that reside on HP-UX servers clone and rdf control of their owned devices.</i>	19
4.3.1 System Requirements	19
4.3.2 Pre-Installation Procedure.....	19
4.3.3 Package Installation.....	19
4.3.4 Post-Installation Procedure	22
5 ADDITIONAL CONFIGURATION	24
5.1 SRDF/A AND SRDF/STAR SPECIFIC CONFIGURATION	24

5.2	ENABLING THE SYMAPI SERVER	24
5.2.1	Introduction	24
5.2.2	SYMAPI server Configuration	24
5.3	ENABLING GROUP NAME SERVICES (“GNS”)	25
5.3.1	Introduction	25
5.3.2	GNS User Authentication	26
5.3.3	Configuring GNS	26
5.3.4	Using GNS	27
5.3.5	Group Name Collisions	28
5.3.6	GNS Backup and Restore	28
5.3.7	GNS remote Mirroring	29
5.4	ENABLING SYMAUTH	29
5.5	AUDIT LOGGING AND ALERTING	33
5.5.1	Configuring the Event Daemon (storevntd)	33
5.6	SANSCREEN CONFIGURATION	34
5.6.1	SYMAPI Server Configuration for SANscreen	34
5.6.2	Symauth Configuration for SANscreen	35
5.7	ECC CONFIGURATION	36
6	BEST PRACTICES	38
6.1	SRDF/A	38
6.2	TIMEFINDER/CLONE	38
6.3	VOLUME LOGIX SUPPORT	38
6.4	VCMDB DATABASE BACKUP	39
6.5	HETEROGENEOUS SERVER SUPPORT	39
6.6	LUN OFFSET	39
6.7	BIN FILE RECONFIGURATION WITH SYMCONFIGURE	41
7	REFERENCES	42
7.1	KEY DOCUMENTATION	42
7.2	RELEVANT SOLUTIONS ENABLER 6.0 DOCUMENTATION SET	43
8	APPENDIX A: VOLUME LOGIC CONVERSION	44
9	APPENDIX B: CERTIFIED SYMCONFIGURE FUNCTIONALITY	45
10	APPENDIX C: RELEASE NOTES	46

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.

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@citi.com.

Latest Versions

It is recommended that the latest version of the document be used from the [GDSE website](#). Newer versions may include expanded scope, or comments on issues discovered after deployment.

Confidentiality

This document is confidential and no part of it should be shared by EMC with any of its other customers.

1 Introduction

The Solutions Enabler ("SE") application from EMC allows configuration and control of the EMC Symmetrix storage arrays. It consists of commands that can be invoked via the command line, or within scripts. The Citigroup standard configuration of Solutions Enabler is installed on a SOE Solaris host that is connected to the Storage Area Network ("SAN"). The application utilizes the fibre channel transport to send commands to the array.

This document serves as a guide for implementation and use of the EMC Solutions Enabler 6.4 application within global Citigroup SAN environments. The information compiled in this document has been tested and certified by Global Distributed Storage Engineering ("GDSE").

1.1 Applicable Environments

SE is used to manage Symmetrix storage arrays. Certain functionality of SE 6.4 might not be available on all Symmetrix hardware types and Enginuity code levels. For a detailed compatibility analysis please refer to the EMC support matrix.

1.2 Release Notes

The SE 6.4 Certification Release Notes can be referenced for detailed information on the scope of the SE 6.4 certification. The Release Notes also contain important information of issues and fixes specific to SE 6.4 as well as the test results for the certification.

2 Certified Features of Solutions Enabler

The following features have been certified for use within Citigroup with SE 6.4. The following features in this section all require 5772 microcode or above.

2.1 SRDF/A Features

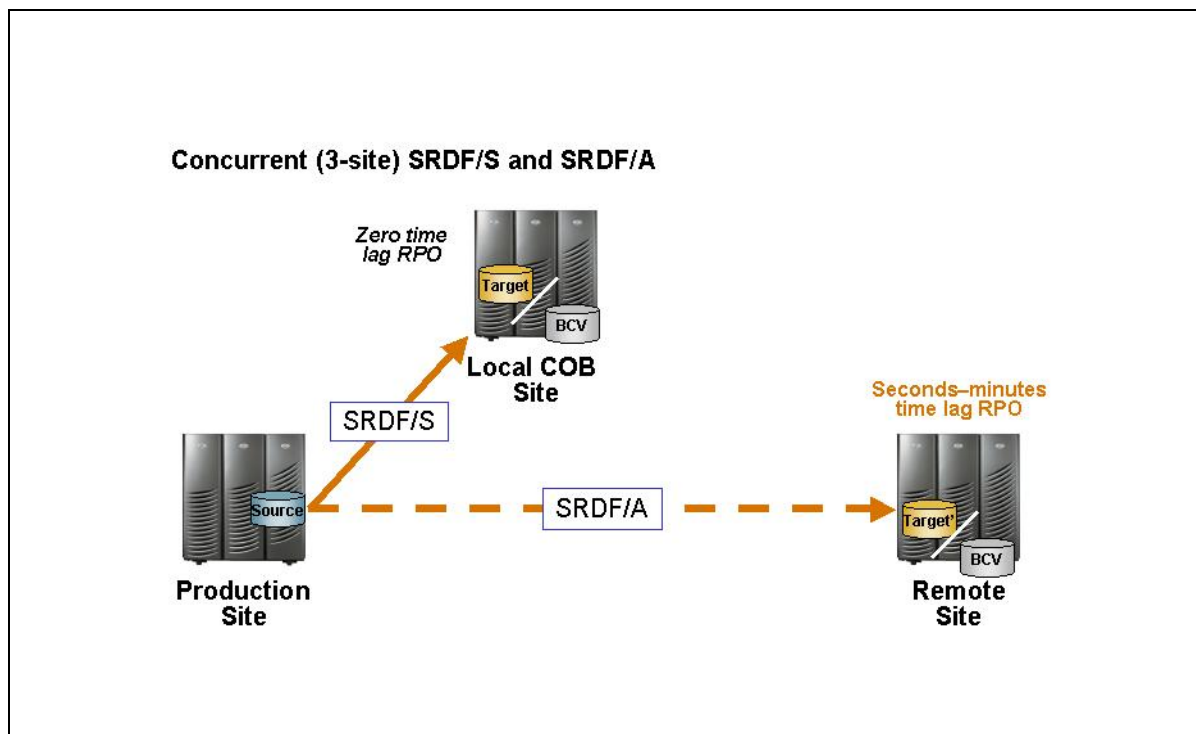
SRDF/Asynchronous (SRDF/A) is a remote mirroring solution for the Symmetrix DMX series. It uses a Delta Set architecture to maintain a consistent point-in-time target (R2) image with only a slight lag behind the source (R1) side, resulting in minimal data loss if the R1 is lost. SRDF/A allows one to configure an SRDF environment in which R1 devices transfer data to R2 devices in chunk cycles. It is suitable for Long Range Replication.

Some key features of the SRDF/A version that has now been certified are highlighted below:

2.1.1 Concurrent SRDF/A and SRDF/S from a single source

This key feature provides the ability to replicate a group of devices in synchronous mode to one target site and in asynchronous mode to a tertiary site at an extended distance. The same source device can be replicated synchronously using SRDF/S mode down one link and asynchronously using SRDF/A down another.

This capability provides a limited multi-site protection capability. In the event of a primary site failure, there would be no data loss since it is synchronously replicated to a local/regional recovery site. In the event of a regional disruption, data has been simultaneously replicated to a recovery site much further away, with minimal potential data loss.



2.1.2 Support for multiple SRDF/A Groups

Multiple SRDF/A sessions (up to 64 depending on configuration) can be configured per DMX array. This allows applications using SRDF/A replication to be managed (e.g. failed over) independently of each other.

2.1.3 Availability

SRDF/A provides a consistent, restartable image at the target site *at all times*, even in the event of a production site outage that results in data loss between R1 and R2. Fast and efficient incremental failback and re-synchronization are also available with SRDF/A.

2.1.4 SRDF/A Write Performance

As writes do not need to be acknowledged by the remote system, there is generally negligible host application IO write response impact regardless of distance between sites (if the solution is properly sized).

2.1.5 Dynamic Pair Operations for SRDF/A

Dynamic control operations can now be performed on SRDF/A capable devices, using the `createpair`, `deletepair`, and `swap` actions of the `symrdf` command.

2.1.6 SRDF/A Statistics Enhancements

Using the `symstat` command, you can check SRDF/A performance statistics, using the `cycle`, `cache`, and `requests` types in conjunction with the `-reptype rdfa` option.

2.2 2-site SRDF/MSC

SRDF/MSC offers the ability to provide SRDF/A replication of multiple RDF groups with I/O consistency across all the groups, whilst still retaining the ability to failover individual RDF groups to deal with, for example, application server failures, without impacting the replication of other applications. MSC allows SRDF/A capable devices to be added to composite groups and enabled for consistency protection.

If one or more source (R1) devices in an SRDF/A consistency group cannot propagate data to their target (R2) devices, the MSC process suspends data propagation from all R1 devices in the consistency group, halting all data flow to the R2 targets.

2.2.1 Multi Session Consistency (MSC) Daemon Support

SRDF/A with MSC is supported by an RDF daemon that performs cycle-switching and cache recovery operations amongst all SRDF/A sessions in the group. It ensures that a consistent R2 data copy of the database exists at the point-in-time any interruption occurs. A composite group must be created using the RDF consistency protection option (`-rdf_consistency`) and must be enabled using the `symcg enable` command before the RDF daemon begins monitoring and managing the MSC consistency group.

The RDF daemon maintains consistency for enabled composite groups across multiple RDF groups for SRDF/A with MSC. For the MSC option (`-rdf_consistency`) to work in an RDF

consistency-enabled environment, each locally-attached host performing management operations must run an instance of the RDF daemon (storrd). Each host must also be running an instance of the base daemon (storapid).

Optionally, if the Group Naming Services (GNS) daemon is also running, it will communicate the composite group definitions back to the RDF daemon. If the GNS daemon is not running, the composite group must be defined on each host individually.

For redundant consistency protection of RDF composite groups, multiple instances of the RDF daemon should be running at the same time on separate hosts. Each host must have a common view of the composite group being monitored. All redundant daemons run simultaneously, monitoring and switching independently of each other. If one of the redundant daemons fails, the other existing daemon(s) will complete the task.

2.2.2 GNS Enhancements

The GNS daemon (storgnsd) can now create remote RDF mirrors for composite groups as well as device groups. For composite groups, only the standard devices are mirrored. In addition, this daemon synchronizes changes to SRDF/MSD consistency groups as it works in companion with the RDF daemon (storrd).

Also with GNS, you can now create and restore backup (shadow) files manually from the command line for attached storage array.

2.2.3 SRDF/MSD

Solutions Enabler Version 6.0 and above supports the creation of RDF-consistent Composite Groups managed via SRDF Multi Session Consistency (SRDF/MSD) using the -rdf_consistency.

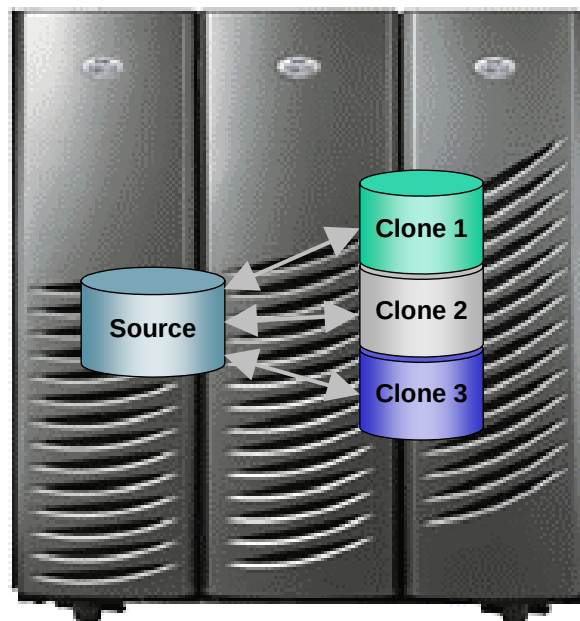
2.3 TimeFinder/Clone

TimeFinder/Clone software for DMX allows one to clone copies of data simultaneously on one or more target devices from a single source device within the same DMX. Data can be copied to as many as 16 target devices (depending on configuration).

TimeFinder/Clone functionality is controlled via copy sessions, which pair the source and target devices. Sessions are maintained on the DMX array and can be queried to verify the current state of the device pairs. A copy session must first be created to define and set up the clone devices. The session is then activated, enabling the target devices to be accessed by its host. When the clone is no longer needed, the session can be terminated. TimeFinder/Clone operations are controlled from the host using the `symclone` commands to `create`, `activate`, `restore`, `split`, `recreate` and `terminate` the copy sessions.

The host controlling the clones will usually be an application server and hence will need a copy of Solutions Enabler installed.

The illustration below shows a single source device with three concurrent copy or clone sessions.



Clones can be created in one of three modes:

PreCopy – Copying of data to the target clone begins as soon as the clone session is created.

Copy – Copying of data to the target clone begins only when the clone is activated

CopyOnAccess – Copy of data to the target clone only occurs after activation and when either data is written to the source or reads or writes take place to the target device.

It is also possible to use TimeFinder/Mirror commands (symmir) to manipulate BCV-based clones when used in clone emulation mode.

3 Installation Preparation

3.1 Host

An SOE Solaris version 8 or 10 host is required to install SE 6.4. The host should be connected to the SAN fabrics to which the Symmetrix storage arrays that are to be managed are connected.

For redundancy, there should be a minimum of two hosts managing the same set of Symmetrix storage arrays. These hosts do NOT require shared storage (clustering configuration) from the SAN; each host should have the Group Name Services enabled to share device group information. Please see [Section 5.3](#) on how the Group Name Service (GNS) is to be configured.

At least two gatekeeper devices should be zoned and masked to the host from every Symmetrix array that is to be managed. Note that gatekeeper device management is now provided by the Base daemon for all SYMAPI/CLI clients that require access to Symmetrix arrays, and for the GNS and RDF daemons. This alleviates contention when there are limited gatekeeper resources available and also eliminates the need for every client to constantly select, open, lock, and ping for an available gatekeeper device for every online function.

If SRDF/MSD is being implemented, then consult the SRDF/A Solutions Guide for additional Gatekeeper requirements.

The SE application can also be installed on hosts running business applications. The SA of such hosts would be able to use Timefinder functionality on the Symmetrix devices assigned to the host without requiring any assistance from the Storage Management Group. At this time, GDSE has only created the SE 6.4 package for Solaris 8/10 and HP-UX 11.11.

3.2 Symmetrix Security

3.2.1 SYMACL Permissions

Symmetrix Host Access Control management (SYMACL) must be used with all Symmetrix to limit host access to Symmetrix control. Before a Solutions Enabler host can issue SYMCLI commands, it should have permissions on each Symmetrix storage array's SYMACL database that it will manage.

SYMACL is initialized by EMC. The SE server's unique ID must be provided to EMC before SYMACL is enabled on the Symmetrix to ensure that it has management access to array after SYMACL is enabled. To get the unique ID for the SE server:

```
# symacl -unique
The unique id for this host is: 2F5802AC-574085CF-993D757A
#
```

Once EMC has enabled SYMACL, the initial symacl list should look like the following:

```
# symacl -sid 919 list -acl
```

Symmetrix ID: 000190100919

Group Name	Pool Name	Access Type
AdminGrp	ALL_DEVS	ALL
AdminGrp	ALL_DEVS	ADMIN
UnknwGrp	ALL_DEVS	Base
UnknwGrp	!INPOOLS	ALL

The initial SE host should already be a member of the AdminGrp accgroup. All SE hosts should be made a member of the SYMACL group called "AdminGrp" on all local and remote Symmetrix arrays that it will manage. The entry in the command file used to add a host to an accgroup is:

```
add host accid 2F5802AC-574085CF-993D757A name sangs6 to accgroup AdminGrp;
```

When executing the command file, the user will be prompted to enter a PIN (the PIN is the the last for digits of the array serial number):

```
# symacl -sid 110 commit -f addhost.cmd
```

Enter Access PIN:

Command file: (addhost.cmd)

PREVIEW.....Started.

PREVIEW.....Done.

PREPARE.....Started.

Adding Host access id sangs5 to group AdminGrp.....Done.

PREPARE.....Done.

Starting COMMIT.....Done.

```
#
```

The accgroup UnknwGrp should be deleted from the symacl list to prevent unauthorized servers from accessing the storage array. The entry in the command file to remove the UnknwGrp is:

```
remove accgroup UnknwGrp remove_aces=true;
```

The Symmetrix service processor will also need symacl entries created for it. The unique ID for the Symmetrix service processor can be obtained from EMC. An accgroup called EMC_SP should be created with VLOGIX, ADMINRD, OPTMZR, and BASE rights to ALL_DEVS. The Symmetrix service processor will need to be added to the accgroup EMC_SP.

The ECC storage agent server will also need symacl entries created for it. Create a group called ECC_HOST and grant it BASE and ECC rights to ALL_DEVS. Add the ECC storage agent server to the ECC_HOST accgroup. See [5.7 ECC Configuration](#).

The final symacl list should look like the following:

```
# symacl -sid 110 list -acl
```

```
Symmetrix ID: 000190103110
```

Group Name	Pool Name	Access Type
-----	-----	-----
AdminGrp	ALL_DEVS	ADMIN
AdminGrp	ALL_DEVS	ALL
EMC_SP	ALL_DEVS	VLOGIX
EMC_SP	ALL_DEVS	ADMINRD
EMC_SP	ALL_DEVS	OPTMZR
EMC_SP	ALL_DEVS	BASE
ECC_HOST	ALL_DEVS	BASE
ECC_HOST	ALL_DEVS	ECC

```
#
```

Note: If symauth is enabled on the storage array (symauth should be enabled on arrays running 5772 or later), only users with the Admin or SecurityAdmin role will be able to make symacl changes. Refer to [5.4 Enabling symauth](#).

3.2.2 VC MDB Access

Before a SAN management server can issue LUN masking commands such as symmask or symmaskdb, it must have access to the VC MDB device for each Symmetrix storage array that it will manage. Application hosts using SE to manage clones will also need to have VC MDB access. Commands required for managing clones will fail with the following message if VC MDB access is not given to the application server:

The gatekeeper device (while using the Base Daemon) has an error (Please see the Log file)

Refer to document [DMX Solutions Guide](#) for further information on configuring VC MDB access for hosts.

3.3 Licensing

Citigroup does not have a blanket license agreement for all components of SE. Hence, only the license keys for basic licensed functions are bundled in the install package. The license keys for the following functionality are provided as a baseline in the default symapi_licenses.dat file:

BASE:	Enables the Base component
Configuration Mgr:	Enables the Symmetrix Configuration Change component.
DevMasking:	Enables the Device Masking component
DeltaMark:	Enabled ChangeTracker
SYMAPI Server:	Enables the Remote SYMAPI Server (network) operations

If you purchased any of your Symmetrix with the Citigroup "High Availability" bundle, then you will also need to install license keys for certain SRDF and TimeFinder products. See the [TimeFinder/Clone Release Notes](#) for details of which license keys are covered by which bundles.

You will need to install any of the following additional license keys¹ that you obtained from EMC for your site by using the “symlmf” SYMCLI command. Alternatively, keys for an existing management server can be edited into the symapi_licenses.dat file.

SRDF or SRDF/Synchronous:	Enables the SRDF component
SRDF/A:	Enables the SRDF/A component
SRDF/DM:	Enables the SRDF/Data Mover component
SRDF/Consistency Groups	Enables SRDF/Consistency Groups (needed for MSC)
TimeFinder/Consistency Group	Enables TF/Consistency Groups
TimeFinder/Mirror:	Enables the TimeFinder (BCV control) component
TimeFinder/Clone:	Enables the TimeFinder (Clone control) component

If the host is being used for SRDF/A control, refer to section “Management Server Configuration” in the document [SRDF/A Solutions Guide](#) for detailed instructions on licensing requirements.

Use of clones (either via symclone commands or via TimeFinder/Mirror Clone Emulation) requires a TimeFinder/Clone license. See the GDSE document [TimeFinder/Clone Release Notes](#) for further details on clone licensing.

¹ Every time one or more license keys are added, the SYMAPI server must be restarted.

4 Installation

4.1 Installing SE 6.4 on Solaris 8 and 10

4.1.1 System Requirements

Minimum amount of disk space needed: 383 MB

Minimum PowerPath Version: v4.5.0

- Run the following command to get the PowerPath version on your system:

```
# powermt version
```

Verify semaphore settings in the /etc/system file (reboot required if changes are made)

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

4.1.2 Pre-Installation Procedure

Before installing the Solutions Enabler software on the server, verify the following:

1. The host has SYMACL permissions on every Symmetrix storage array that it will manage.
2. The host must be properly zoned to the Symmetrix storage array that it will manage. Once zoned, the host should be configured to see the VC MDB device (e.g. For Solaris 8 hosts, persistent bindings set in lpfc.conf and entries to discover LUN 0 in sd.conf).

4.1.3 Package Installation

1. If this is an upgrade, run the following command to update the configuration database:

```
# symcfg discover
```

If this is a new installation, proceed to Step 9 in this section.

2. Create a backup of the VC MDB:

```
# symmaskdb -sid SymmID backup -file BackupFilename
```

3. Check to see if GNS is enabled on the server by looking in the options file in the /var/symapi/config directory. If not, ensure that device groups and composite groups defined on this server are restored after Solutions Enabler is upgraded. See the post-installation instructions for the procedure.
4. Stop all Solutions Enabler daemons:

stordaeon shutdown all -immediate

5. Stop the symapi server:

symapisrv stop

6. Make a backup copy of the **/var/symapi/db** directory:

find /var/symapi/db -print -depth|cpio -pcvmud /var/tmp/symapi_bk/db_old

7. Make a backup copy of the **/var/symapi/config** directory:

find /var/symapi/config -print -depth|cpio -pcvmud /var/tmp/symapi_bk/config_old

8. Perform a backup of the system if possible.
9. Run the following commands to create the installation directory:

```
# mkdir /export/opt/emc
# cd /opt
# ls emc
```

10. Run the install script on the network share:

```
# cd /net/stealth/export1/home1.localhost/sw/PKG/emcsolen642
# ./se6423 install.sh --install
```

```
#-----
#           EMC Installation Manager
#-----
Copyright 2007, EMC Corporation
All rights reserved.
```

The terms of your use of this software are governed by the applicable contract.

Solutions Enabler Native Installer[RT] Kit Location :
/net/stealth/export1/home1.localhost/sw/PKG/emcsolen642

Install root directory of previous Installation : **/opt/emc**
Do you want to change Install root Directory. [N] :
Install root directory : **/opt/emc**
Working root directory : **/usr/emc**

Checking for OS version compatibility.....
Checking for previous installation of Solutions Enabler.....
Checking for previous installation version.....

There is a previous version of SYMCLI installed on this host
named [/opt/emc/SYMCLI/V6.4.2]
Do you want to save /SYMCLI/V6.4.2? [N]:**n**

Checking for active processes.....
Checking for /usr/symcli/storbin/cimserver...
Checking for /usr/symcli/bin/symapisrv...

Checking for active SYMCLI components...

Install All EMC Solutions Enabler Shared Libraries and Run Time Environment ? [Y]:y
Install EMC Solutions Enabler 64-bit Shared Libraries ? [N]:n
Install Symmetrix Command Line Interface SYMCLI ? [Y]:y
Install EMC Solutions Enabler SRM Database Run Time Components ? [N]:y
SRM ORACLE Database Components ? [N]:n
SRM INFORMIX Database Components ? [N]:n
SRM SYBASE Database Components ? [N]:n
SRM UDB Database Components ? [N]:n
Install Option to Enable JNI Interface for EMC Solutions Enabler APIs ? [N]:n
Install Option to Enable EMC Solutions Enabler Star Component ? [N]:y
Install Option to Enable EMC Solutions Enabler SYMRECOVER Component ? [N]:y

Do you want to change default permission on /var/symapi directory from [755]? [N]:y

Valid permission mask for /var/symapi directory is [7][01457][01457].

Enter the permission mask to be set for /var/symapi directory :775

Checking for disk space availability....

Persistent data files exist in directory[/usr/emc/API/symapi]...

Do you want to MOVE this data to /usr/emc/API/symapi_old? [N]: n

Uninstalling previous installation of Solutions Enabler.
It may take some time. Please wait...

Uninstallation of previous installation of Solutions Enabler was successful.
A copy has been saved to [/opt/emc/SYMCLI/symcli_old].

Non interactive installation using pkgadd.

Installing SYMdcore.....

Installing SYMdbase.....

Installing SYMcore.....

Installing SYMstrbse.....

Installing SYMstrful.....

Installing SYMsrbse.....

Installing SYMsymcli.....

Installing SYMstarp.....

Installing SYMsymrec.....

The previous version of SYMCLI that was saved during this installation now exists in [/opt/emc/SYMCLI/symcli_old]
 Do you want to remove the symcli_old directory [y]: **n**
 Enabling stordaemon...

Do not forget to run 'symcfg discover' if this is your first install or whenever your configuration changes.

You may need to manually rediscover remotely connected arrays. Please see the installation notes for more information.

```
#-----
# The following HAS BEEN INSTALLED in /opt/emc via the pkgadd utility.
#-----
ITEM  PRODUCT                                VERSION
01   EMC Solutions Enabler                    V6.4.2.3
      RT KIT
#-----
```

4.1.4 Post-Installation Configuration

1. Set the following in the **.profile** file:

```
PATH=$PATH:/usr/storapi/bin:usr/storapi/storbin:.
MANPATH=$MANPATH:/usr/storapi/man:/usr/storapi/storman
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/storapi/shlib:.
export PATH MANPATH LD_LIBRARY_PATH
```

2. The **symapi_licenses.dat** file should be created in the **/var/symapi/config** directory with the following entries (if this was an upgrade, the prior symapi_licenses.dat file should've been preserved):

```
# cat symapi_licenses.dat
License Key: 7FBE-9150-E0BC-9CCD SYMAPI Feature: BASE / Symmetrix
License Key: C7B7-B992-1954-4D99 SYMAPI Feature: DeltaMark / Symmetrix
License Key: A97E-6602-DABA-9E2A SYMAPI Feature: DevMasking / Symmetrix
License Key: A936-39CD-A0FF-CDC5 SYMAPI Feature: ConfigChange / Symmetrix
```

3. If any additional licenses need to be registered, run the following command to register them:

```
# symlmf
```

4. Assign gatekeepers and vcm device to the server if that hasn't already been done.
5. Run the following command to build the configuration (SYMAPI) database:

```
# symcfg discover
```

4.2 Backing Out of an Upgrade

If it is needed to back out of a SE upgrade, do the following:

1. Verify that a backup copy of the old version in the **/opt/emc/SYMCLI/symcli_old/** directory.
2. Uninstall the current version of the SE:
3. Install the prior version of SE that was installed on the server before the upgrade.
4. If GNS was not enabled on the server, copy the backup copy of the SYMAPI database into the **/var/symapi/db**
5. Copy the old **symapi_licenses.dat** file back to the **/var/symapi/db** directory:

```
# cp /var/tmp/symapi_bk/config_old/var/symapi/config/symapi_licenses.dat
/var/symapi/config
```

6. Copy the backup copy of the **options** and **daemon_options** file back to the **/var/symapi/config** directory.
7. Run the following command to rebuild the configuration (SYMAPI) database:

```
# symcfg discover
```

4.3 Installing SE 6.4 on HP-UX 11.11

HP-UX is not the standard management platform for the Symmetrix within Citi. This package for HP-UX servers is to provide special applications that reside on HP-UX servers clone and rdf control of their owned devices.

4.3.1 System Requirements

Minimum amount of disk space needed: 360MB

Minimum PowerPath Version: v4.5.0

- Run the following command to get the PowerPath version on your system:

```
# powermt version
```

4.3.2 Pre-Installation Procedure

Before installing the Solutions Enabler software on the server, verify the following:

1. The host has SYMACL permissions on each of the Symmetrix storage array's SYMACL database that it will manage.
2. The host should have access to the VCMDDB of each of the Symmetrix storage arrays that it will manage.

4.3.3 Package Installation

1. If this is an upgrade, run the following command to update the configuration database:

```
# symcfg discover
```

If this is a new installation, proceed to Step 9 in this section.

2. Create a backup of the VCMDDB:

- # symmaskdb -sid SymmID backup -file BackupFilename**
3. Check to see if GNS is enabled on the server by looking in the options file in the /var/symapi/config directory. If not, ensure that device groups and composite groups defined on this server are restored after Solutions Enabler is upgraded. See the post-installation instructions for the procedure.
 4. Stop all Solutions Enabler daemons:
stordaeon shutdown all -immediate
 5. Stop the symapi server:
symapisrv stop
 6. Make a backup copy of the /var/symapi/db directory:
find /var/symapi/db -print -depth|cpio -pcvmud /var/tmp/symapi_bk/db_old
 7. Make a backup copy of the /var/symapi/config directory:
find /var/symapi/config -print -depth|cpio -pcvmud /var/tmp/symapi_bk/config_old
 8. Perform a backup of the system if possible.
 9. Go to the **hpsolen6423** directory on the network share:
cd /net/stealth.nj.ssmb.com/export1/home1.localhost/sw/HP-UX/hpsolen6423
 10. Run the installation script:
uclabhp6# ./se6423_install.sh -install

#-----

EMC Installation Manager
#-----

Copyright 2007, EMC Corporation
All rights reserved.

The terms of your use of this software are governed by the
applicable contract.

Solutions Enabler Native Installer[RT] Kit Location : /rootgdse/ql68074/se64/software/SYMCLI.depot

Install root directory [/opt/emc] : <cr>
Working root directory [/usr/emc] : <cr>

Checking for OS version compatibility.....
Checking for previous installation of Solutions Enabler.....
Checking for previous installation version.....

There is a previous version of SYMCLI installed on this host
named [/opt/emc/SYMCLI/V6.3.0]

Do you want to save /SYMCLI/V6.3.0? [N]: **<cr>**

Checking for active processes.....

Checking for /usr/symcli/storbin/cimserver...

Checking for /usr/symcli/bin/symapisrv...

Checking for active SYMCLI daemons...

Checking for active SYMCLI components...

PID	TTY	TIME	COMMAND
4936	?	0:01	mhragent

WARNING: The above processes may prevent the completion of this INSTALL.

Selecting Kill option may kill other applications which are using Soluti
on Enabler Components.

Do you want to kill above Processes [Y] or Exit INSTALL [X]? [Y] : **y**

Killing the above processes. It may take some time...

Working root directory changed from to /usr/emc.

Install All EMC Solutions Enabler Shared Libraries and Run Time Environment ? [Y]: **<cr>**

Install EMC Solutions Enabler 64-bit Shared Libraries ? [N]: **<cr>**

Install Symmetrix Command Line Interface SYMCLI ? [Y]: **<cr>**

Install EMC Solutions Enabler SRM Database Run Time Components ? [N]:**y**

SRM ORACLE Database Components ? [N]: **<cr>**

SRM INFORMIX Database Components ? [N]: **<cr>**

SRM SYBASE Database Components ? [N]: **<cr>**

SRM UDB Database Components ? [N]: **<cr>**

Install Option to Enable JNI Interface for EMC Solutions Enabler APIs ? [N]: **<cr>**

Install Option to Enable EMC Solutions Enabler Star Component ? [N]:**y**

Install Option to Enable EMC Solutions Enabler SYMRECOVER Component ? [N]:**y**

Do you want to change default permission on /var/symapi directory from [755]? [N]:**y**

Valid permission mask for /var/symapi directory is [7][01457][01457].

Enter the permission mask to be set for /var/symapi directory :**775**

Checking for disk space availability....

Uninstalling previous installation of Solutions Enabler.

It may take some time. Please wait...

Uninstallation of previous installation of Solutions Enabler was successful.

Creating fileset list for installation.

It may take a few minutes

Following data filesets will be installed:

1. SYMCLI.DATACORE

2. SYMCLI.DATASTORBASE

Installing SYMCLI data files...

Following SYMCLI filesets will be installed:

1. SYMCLI.CORE
2. SYMCLI.STORBASE
3. SYMCLI.STORFULL
4. SYMCLI.SRMBASE
5. SYMCLI.SYMCLI
6. SYMCLI.STAR_PERL
7. SYMCLI.SYMRECOVER

Installing SYMCLI fileset. It will take a few minutes.....

Creating OPENSSL Certificate....

Enabling stordaemon...

Do not forget to run 'symcfg discover' if this is your first install or whenever your configuration changes.

You may need to manually rediscover remotely connected arrays. Please see the installation notes for more information.

```
#-----
# The following HAS BEEN INSTALLED in /opt/emc via the swinstall utility.
#-----

ITEM  PRODUCT                                VERSION
01   EMC Solutions Enabler                  V6.4.2.3
     RT KIT
#-----
```

4.3.4 Post-Installation Procedure

1. Set the following in the **.profile** file:

```
PATH=$PATH:/usr/storapi/bin:usr/storapi/storbin:.
MANPATH=$MANPATH:/usr/storapi/man:/usr/storapi/storman
export PATH MANPATH
```

2. Create the **symapi_licenses.dat** file in the **/var/symapi/config** directory and input the following entries into that file (if this was an upgrade, the symapi_licenses.dat file should've been preserved):

```
License Key: 7FBE-9150-E0BC-9CCD SYMAPI Feature: BASE / Symmetrix
License Key: C7B7-B992-1954-4D99 SYMAPI Feature: DeltaMark / Symmetrix
```

License Key: A97E-6602-DABA-9E2A SYMAPI Feature: DevMasking / Symmetrix
License Key: A936-39CD-A0FF-CDC5 SYMAPI Feature: ConfigChange / Symmetrix

3. If any additional licenses need to be registered, run the following command to register them:

symlmf

4. Set the proper parameters in the **options** and **daemon_options** file in the **/var/symapi/config** directory. DO NOT replace the new options file with the backup copy. Doing so will result in missing feature settings included in the new options file. The old files can be referenced to configure the parameters in the new files.
5. Assign gatekeepers to the server and vcm device to the server if that has not been done yet.
6. Run the following command to build the configuration (SYMAPI) database:

symcfg discover

5 Additional Configuration

5.1 SRDF/A and SRDF/Star Specific Configuration

If the host is being used for SRDF/A control, refer to section “Management Server Configuration” in the [SRDF/A Solutions Guide](#) and [SRDF/Star Solutions Guide](#) for detailed instructions on additional host configuration steps.

5.2 Enabling the SYMAPI Server

5.2.1 Introduction

The SYMAPI server that runs on the SE server and provides a method for a client server that doesn't have fibre channel access to the storage array to manage the array. The client server connects to the SE server's SYMAPI server via the TCP/IP network to issue SYMCLI commands. These commands are then executed via fibre channel from the SE server to the array.

The use of the SYMAPI server should be limited to SANscreen servers only. SE management servers should have a fibre channel connection to the array, therefore, the SE management servers do not need to use the SYMAPI server when managing the storage array.

5.2.2 SYMAPI server Configuration

Note that a separate license is needed for SYMAPI server and is not covered by the Base license key. This additional key is included in the license file in the Solaris package.

This is how the SYMAPI server functionality is to be enabled:

On the client server (e.g. SANscreen server), add the following to the `/var/symapi/config/netcnfg` file:

```
SYMAPI_SERVER      -      TCP/IP      -      <SE server's IP address>      2707
```

For example:

```
SYMAPI_SERVER      -      TCP/IP      -      169.193.70.169      2707      -
```

This instructs SYMCLI commands to connect to the SE server's SYMAPI server.

To specify which hosts on the TCP/IP network can use the SYMAPI server, the “nethost” file has to be configured on the SE server. If it does not already exist, create the edit `/var/symapi/config/nethost` file and add:

```
<this-host-IP-address>  <username>
```

where <username> is the login id of an authorized member of the SAN management team.

For example:

```
169.193.70.169      *      #SANscreen requires the (*) as the user.
```

The SYMAPI server should now be started with:

```
# stordaeon start storsrvd
```

This command should be made into a script and installed such that it is executed every time the system boots up. For example, file /etc/rc3.d/S999emc_symapisrv could contain

```
#!/sbin/sh
echo "Starting SYMAPI server"
/usr/symcli/bin/stordaeon start storsrvd
exit $?
```

Only authorized storage operators should be configured to log on to the host². 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)³.

Each storage operator's account should be profiled with the following:

The following should be added to each user's profile file on the client server:

```
PATH=$PATH:/usr/storapi/bin;usr/storapi/storbin
MANPATH=$MANPATH:/usr/storapi/man:/usr/storapi/storman
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/storapi/shlib
SYMCLI_CONNECT=SYMAPI_SERVER
export PATH MANPATH LD_LIBRARY_PATH SYMCLI_CONNECT
```

The "SYMCLI_CONNECT" environment variable should only be set to "SYMAPI_SERVER" on the SE client server and NOT on the SE server. This will force the SYMCLI commands to use the SYMAPI server for executing the commands, instead of directly using the SYMCLI libraries⁴.

The command '**symcli -def**' will show if this environment variable has been set.

5.3 Enabling Group Name Services ("GNS")

5.3.1 Introduction

In a pre-SE5.5 Symmetrix environment, device group and composite group definitions are created via a locally attached host. Upon creation, the group definition is stored in the host's configuration database file. Therefore, only the host that created the group would see the group and control it. To perform control operations from another locally attached host, the group definition would have to be manually copied to other hosts.

GDSE certified GNS with the release of SE 5.5. GNS provides the ability to store device and composite group definitions in a shared repository located on each Symmetrix array, which would then automatically become visible to all hosts that are configured to run Solutions Enabler. This

² GDSE does not recommend sharing hosts that are used to manage storage with other applications for security reasons. At this time SYMACL can only restrict access by host, and not by individual user IDs.

³ These are information security requirements. This will allow for tracking of storage operator activity with a new application that GDSE is developing.

⁴ EMC does not support running of SYMCLI commands from an unprivileged ("non root") user account. GDSE is proposing the use of the SYMAPI server as a workaround.

allows all GNS-enabled hosts to see the same group definitions across the Symmetrix environment, while sharing real-time updates to group definitions and configurations made by other hosts.

As of SE 6.0, the GNS daemon (storgnsd) can now create remote RDF mirrors for composite groups as well as device groups. For composite groups, only the standard devices are mirrored. In addition, this daemon synchronizes changes to SRDF/MSR consistency groups as it works in companion with the RDF daemon (storrdtd).

Also with SE 6.0 or above, GNS you can now create and restore backup (shadow) files manually from the command line for attached storage array.

The present document only covers basic GNS configuration. However, the EMC Engineering White Paper **“Using SYMCLI and GNS to propagate Group Definition to Multiple Hosts”** gives an excellent summary of GNS operations, with examples, and is recommended reading when enabling GNS.

5.3.2 GNS User Authentication

GNS is intended to share group definitions across multiple users and hosts in a Symmetrix environment via the host installed GNS daemons. As such, limiting permission to the GNS daemon controls access to GNS functionality. However, this type of permission control is **NOT** required in the Citigroup environment because all users logging on to the SOE host have same storage management responsibilities (and therefore need the same privileges).

5.3.3 Configuring GNS

If the daemon_options file does not already exist, copy the template README.daemon_options file to /var/symapi/config/daemon_options and edit. The following options should be set:

Option	Description
storgnsd:autorestart=enable	Make use of the watchdog mechanism to automatically restart the daemon if it crashes.
storgnsd:gns_device_poll_interval=15	The interval, in seconds, at which to poll locally-attached Symmetrix arrays for group changes.
storgnsd:gns_device_remote_poll_interval=60	The interval, in seconds, at which to poll remotely-attached Symmetrix arrays for group changes.
storgnsd:gns_rmtarr_update_interval=1000	Interval in seconds to use to check for group changes that need to be propagated to remote Symmetrix arrays. The default is 60 seconds.
storgnsd:gns_syndiscover_interval=600	The interval, in seconds, at which to check for Symmetrix configuration changes.
storgnsd:gns_ppath_poll_interval=60	The interval, in seconds, at which to check whether PowerPath definitions need to be updated.
storgnsd:gns_shadow_file=enable	If set to enable, the daemon automatically

	maintains backup copies of GNS data for locally attached Symmetrix arrays. These backups, maintained on the local disk, are automatically restored to the GNS repository on an array if the daemon detects that a repository has been erased (for example, in the event of a power failure under Enginuity 5x67 or 5x66).
--	---

5.3.4 Using GNS

To instruct SYMCLI to use GNS instead of the local SYMAPI database, edit the `/var/symapi/config/options` file, and uncomment the following line:

```
SYMAPI_USE_GNS=ENABLE
```

GNS daemon `storgnsd` will need restarting.

Stop the daemon with the command

```
# stordaeon shutdown storgnsd
```

The GNS daemon is started automatically when a SYMCLI command that manipulates groups, such as `symdg`, is issued.

Alternatively, the daemon can be started manually via the `stordaeon` command line utility as follows:

```
# stordaeon start storgnsd
```

In addition, the daemon can be set to start automatically every time the local host is booted using the following command line:

```
# stordaeon install storgnsd -autostart
```

Pre-starting the daemon, either manually or via the automatic option, is useful because the daemon may take a while to initially construct its cache — depending on the number of groups and Symmetrix arrays it has to load.

If the daemon is stopped for some reason, it can optionally be restarted automatically by an internal Solutions Enabler watchdog mechanism. A combination of the watchdog mechanism and the auto-start option described above can be used to ensure that the daemon is always running.

Any existing group definitions should now be imported to GNS with the following commands:

```
# symdg activateall
# symcg activateall
```

To see if a group has been imported successfully, you can use the `symdg show DgName` or `symcg show CgName` commands. The output should have “Device Group in GNS : Yes” added to it.

GNS is now ready for use. Group definitions can now be created, edited or deleted as before with `symdg` and `symcg` SYMCLI command. All modifications will automatically be applied to the GNS database on the Symmetrix. The local database will not be used.

The GNS daemon (storgnsd) can now create remote RDF mirrors for composite groups as well as device groups. For composite groups, only the standard devices are mirrored. In addition, this daemon synchronizes changes to SRDF/MSC consistency groups as it works in companion with the RDF daemon (storrdfd). This is covered in a separate subsection.

5.3.5 Group Name Collisions

Each GNS daemon attempts to ensure that group names are unique (relative to a group type). It is possible, however, for duplicate named groups to occur. For example, it is possible for two different groups to be created with the same name on different Symmetrix arrays. A subsequent reconfiguration could then allow the GNS daemon to see both groups. If a GNS daemon detects duplicate group names, it returns a state flag informing clients of this fact and modifies the group names to be unique by attaching a numeric suffix. For example, duplicate device groups with the name MyDG could be modified in the following way:

```
MyDG#12345678  
MyDG#87654321
```

While in this state (duplicate names), the only operations permitted on them are those that can be used to resolve the name conflict: group rename and delete (with the -force flag). For example:

```
# symdg delete MyDG#12345678 -force  
# symdg rename MyDG#87654321 MyDG
```

5.3.6 GNS Backup and Restore

GNS group definitions are stored within the each individual Symmetrix array. These definitions can be lost if a Symmetrix is completely re-initialized or power is lost on a Symmetrix running Enginuity 5x66 or 5x67. A GNS daemon can be configured to automatically backup and restore GNS data from individual arrays. When backup is enabled, the daemon will write an image of the GNS group information to the host's local disk each time it makes a change or it notices a change made from another locally attached host. These backups are maintained as separate per-Symmetrix files and named SymmID.shadow within the /var/symapi/gns/ directory on the host machine⁵.

Automatic backup of the GNS database should be enabled by setting the storgnsd:gns_shadow_file=enable option in the /var/symapi/config/daemon_options file.

As of SE6.0, you can also now create and restore backup (shadow) files manually from the command line for attached storage array. For example:

```
# /usr/symcli/daemons/storgnsd backup -sid <SID>  
# /usr/symcli/daemons/storgnsd restore -sid <SID>
```

Note, however, that automatic backups and manual backups write to the same shadow file. Consequently, if you want to preserve a manual backup made at a particular time, you should make a copy of the shadow file (/var/symapi/gns/SID.shadow) after the manual backup is completed.

⁵ Because the maintenance of numerous backup images can impact performance, it is recommended that you do not enable it on all GNS daemons. Typically, it is recommended that you configure a maximum of 2 GNS daemons to maintain backups for each Symmetrix array that may hold GNS data.

5.3.7 GNS remote Mirroring

As of the SE 6.0 release, GDSE is supporting mirroring of RDF Group Definitions in a Remote Symmetrix Array.

With remote mirroring, GNS will automatically maintain a mirrored group definition on the remote Symmetrix array. This mirroring of groups converts a local RDF1 type group to a remote RDF2 type group, and vice versa. Also local BCVs are converted to remote BCVs and vice versa.

When changes are made to the local group definition, GNS automatically propagates corresponding change to the remote group definition, keeping the two groups synchronized. The remote mirrored group has the same name as the local group and has a mirror image of its contents, bar those elements that are swapped such as the RDF type.

To enable mirroring of an RDF group definition, set the following option in the GNS daemon options file.

```
storgnsd:gns_remote_mirror=enable
```

By default, mirrored groups are read-only and cannot be modified or renamed. The default behaviour is recommended at this time.

Note that propagation of group definitions is controlled by the daemon_options file entry

```
storgnsd:gns_device_remote_poll_interval=60
```

Hence, it may take a minute or so before the definition is visible at the remote site.

GNS remote mirroring is not supported for device groups containing Concurrent SRDF devices.

For further information on remote mirroring, refer to the EMC Engineering White Paper “**Using SYMCLI and GNS to propagate Group Definition to Multiple Hosts**”.

5.4 Enabling symauth

User-based access control is now available with Solutions Enabler 6.4 and Symmetrix arrays running 5772 code or later. The operating system's users on the Solutions Enabler server are to be assigned ONE role out of five possible roles. It is not possible to assign more than one role to a user. These roles are:

- **Monitor** – Read-only role but cannot read the symaudit log or symacl entries.
- **StorageAdmin** – Able to perform all storage management functions except for security functions (i.e. symacl, symauth, and symaudit). Currently, the StorageAdmin cannot view symacl and symaudit information but can view symauth information.
- **Admin** – Able to perform all functions.

- **SecurityAdmin** – Able to perform all symacl, symauth, symaudit, and all Monitor functions.
- **Auditor** – Able to view but not modify symacl, symauth, and symaudit functions. Can also perform all Monitor functions.

Before enabling symauth on the storage array, the symauth entries should be created for all users who will be managing/monitoring the storage array. At the very least, the following users should be entered into the symauth list: SecurityAdmin and StorageAdmin.

To create symauth user entries on the array:

1. Ensure that symauth is disabled on the array:

```
# symauth -sid 110 list
```

```
SYMMETRIX AUTHORIZATION STATUS
```

```
Symmetrix ID: 000190103110
```

```
Authorization Control      : Disabled
```

```
Time Enabled              : N/A
```

```
Time Disabled             : N/A
```

```
Time Updated              : N/A
```

```
Enforcement Mode          : Enforce
```

```
Server Policy              : Trust clients
```

```
#
```

2. Create a command file called **adduser.cmd** with the following entries:

```
assign user H:sangs7\sw54321 to role SecurityAdmin;
```

```
assign user H:sangs7\cp12345 to role StorageAdmin;
```

The user name of the entry is comprised of three parts:

1. **H:** or **D:**. If it starts with a **H:**, that specifies that the user was authenticated by the host system. If it starts with a **D:**, it means the user is authenticated by a domain. In the example above, the users are authenticated by a host system so **H:** is used.
2. The next part of the user name is the hostname the server or the domain name that user is logged into. In the example above, the users are authenticated by the host system **sangs7**.
3. The last part is the user name of the user (this should be the user's SOEID). In the example above, the user **sw54321** on host **sangs7** was assigned the role of **SecurityAdmin**.

Note: An easy way to find out what to use for the host's username is to look into the symapi log to see what Solutions Enabler sees as the username for the user trying to access the array without the proper permissions. Just issue a symcli command to the array and an error should appear in the symapi log for that host since a symauth

entry has not been created for it. An error similar to the one shown below should appear in the log, notice the user name in bold:

```
5-v440-01\root] [host=f5-v440-01] [actid=SE3f9a80cedd] [appid=SYMCLI] [aud-
cls=Security] [aud-act=Denied] [aud-num=3598] = Access Denied for User H:f5-
v440-01\root, access BASE (minimum necessary Role: Monitor)
```

3. After the command file is create, execute the command file with the **symauth** command:

```
# symauth -sid 110 preview -f adduser.cmd

PREVIEW.....Started.
PREVIEW.....Done.
# symauth -sid 110 commit -f adduser.cmd

Perform an Authorization change on Symmetrix unit 000190103110 (y/[n]) ? y

PREVIEW.....Started.
PREVIEW.....Done.

COMMIT.....Started.
assign user H:sangs7\sw54321 to role SecurityAdmin.....Done.
assign user H:sangs7\cp12345 to role StorageAdmin.....Done.
COMMIT.....Done.
#
```

4. Verify the user entries:

```
# symauth -sid 110 list -users

SYMMETRIX AUTHORIZATION USERS

Symmetrix ID: 000190103110

Role name      Username
-----
SecurityAdmin   H:sangs7\sw54321
StorageAdmin    H:sangs7\cp12345
#
```

5. The users with the StorageAdmin role will need to have **rw-** access to the files **symapi_db.bin** and **symapi_licenses.dat**. The permissions to the file will need to be changed to allow **rw-** access to the owner and group.

```
# setfacl -m user:cp12345:rw- symapi_licenses.dat
# chmod 775 symapi_licenses.dat
# setfacl -m user: cp12345:rw- symapi_db.bin
# chmod 775 symapi_db.bin
```

6. Modify the **/var/symapi/config/daemon_users** file to allow the alternate users to use the daemons. This needs to be entered for all users using SE:

```
cp12345      stor*
sw54321      stor*
```

7. Once all of the symauth user entries are entered on both the local and remote storage arrays (symauth entries must be also be created for the remote arrays for SRDF functionality), enable symauth on the Symmetrix:

```
# symauth -sid 110 enable
```

```
Perform an Authorization change on Symmetrix unit 000190103110 (y/[n]) ? y
#
```

8. Verify that the **Enforcement Mode** is set to **Enforce**:

```
# symauth -sid 110 list
```

SYMMETRIX AUTHORIZATION STATUS

```
Symmetrix ID: 000190103110
```

```
Authorization Control      : Enabled

Time Enabled              : Thu Dec 6 11:03:05 2007
Time Disabled             : N/A
Time Updated              : Thu Dec 6 11:03:05 2007

Enforcement Mode          : Enforce
Server Policy             : Trust clients
```

```
#
```

If it is not set to **Enforce**, then set the mode by:

```
# symauth -sid 110 enable
```

```
Perform an Authorization change on Symmetrix unit 000190103110 (y/[n]) ? y
#
```

5.5 Audit Logging and Alerting

SE 6.4 can only read the symaudit logs of a Symmetrix array running 5772 code due to a new audit log repository implemented in 5772 code. The symaudit log entries can be viewed by issuing the 'symaudit' command. If symauth is enabled on the Symmetrix, the user issuing the symaudit command must have the role of SecurityAdmin, Auditor, or Admin.

5.5.1 Configuring the Event Daemon (storevntd)

The SE event daemon (storevntd) is a daemon that runs on the SE server and can be used to import the symaudit log as well as to send out Symmetrix alerts via snmp, syslog, the OS's event log, or to a file. The following steps should be followed to configure the storevntd:

1. The following are the main entries should reside in the /var/symapi/config/daemon_options file on the SE server to specify the behaviour of the storevntd (There are some other parameters in the daemon_options file for the storevntd but the following are the basic settings to get storevntd to functioning):

```
storevntd:log_event_targets = file #Specifies to direct the logs and events to a local file.

storevntd:log_symmetrix_events = \
    sid=000190100919, audit, tgt=file;\ #Directs symaudit logs from the specified
Symmetrix to the local file.
    status, tgt=file;\ #Directs Symmetrix status messages to the local file.
    events, tgt=file #Directs Symmetrix events to the local file.

storevntd:log_event_file_name = symevents #specifies the name of the log file.
```

2. Add a symauth entry for storevntd. In the example below, a command file called **adduser.cmd** was created with the entry **assign user H:sangs7\storevntd to role Auditor**; to create the symauth entry for storevntd:

```
# symauth -sid 110 commit -f adduser.cmd
```

Perform an Authorization change on Symmetrix unit 000190103110 (y/[n]) ? y

```
PREVIEW.....Started.
```

```
PREVIEW.....Done.
```

```
COMMIT.....Started.
```

```
assign user H:sangs7\storevntd to role Auditor.....Done.
```

```
COMMIT.....Done.
```

```
#
```

3. Start storevntd:

```
# stordaeon start storevntd
```

Waiting for daemon to start. This may take several seconds.

```
#
```

4. Run the command to have storevntd start automatically after a system reboot:

```
# stordaeon install storevntd -autostart
```

5. Reload the new options specified in the daemon_options file for the storevntd:

```
# stordaeon action storevntd -cmd reload
```

```
storevntd          Action performed
```

```
#
```

The symaudit events stored in the log file generated by storevntd can now be exported to eTrust for log consolidation and reconciliation. Please reference the [eTrust Solutions Guide](#) for eTrust configuration.

5.6 SANscreen Configuration

SANscreen is an application used to monitor, analyze, and validate changes in the SAN. The SANscreen server and application will need to have the correct access to the SE server and the storage array (i.e. SYMAPI client/server configuration and symauth). This section will cover what needs to be configured on the SE server and the storage array to enable SANscreen to monitor the Symmetrix.

5.6.1 SYMAPI Server Configuration for SANscreen

SANscreen server needs to be given permission to initiate commands via the SE server's SYMAPI server.

Do the following on the SE server:

1. In the **/var/symapi/config/nethosts** file, add an entry for the SANscreen server (an asterisk should be specified as the username):

For example: 10.40.42.37 *

- Restart the SYMAPI server:

```
# stordaeon shutdown storsrvd
storsrvd          Told to shutdown
Waiting for daemon(s) to shutdown. This may take several seconds.
# stordaeon start storsrvd
Waiting for daemon to start. This may take several seconds.
#
```

- Ensure that the SYMAPI server daemon (storsrvd) is running:

```
# stordaeon list

Available Daemons ('[*]': Currently Running):

[*] storapid      EMC Solutions Enabler Base Daemon
[*] storgnsd      EMC Solutions Enabler GNS Daemon
[*] storrdfd      EMC Solutions Enabler RDF Daemon
[*] storevntd     EMC Solutions Enabler Event Daemon
[*] storwatchd    EMC Solutions Enabler Watchdog Daemon
storsrmd          EMC Solutions Enabler SRM Daemon

stororad          EMC Solutions Enabler SRM Oracle Daemon
storora64d        EMC Solutions Enabler SRM Oracle Daemon, 64-bit
storudbd          EMC Solutions Enabler SRM UDB Daemon
storudb64d        EMC Solutions Enabler SRM UDB Daemon, 64-bit
storifmxd         EMC Solutions Enabler SRM Informix Daemon
storifmx64d       EMC Solutions Enabler SRM Informix Daemon, 64 bit
storsybs12d       EMC Solutions Enabler SRM Sybase 12 Daemon
storsybs12.5d     EMC Solutions Enabler SRM Sybase 12.5 Daemon
storsybs12.5_64d  EMC Solutions Enabler SRM Sybase 12.5 Daemon, 64-bit
storstpd          EMC Solutions Enabler STP Daemon
[*] storsrvd      EMC Solutions Enabler SYMAPI Server Daemon

#
```

Refer to the [SANscreen Solutions Guide](#) to configure the SANscreen server to use the SE server's SYMAPI server.

5.6.2 Symauth Configuration for SANscreen

Create a symauth entry for the SANscreen server and application. Use the **D:NT AUTHORITY\SYSTEM** as the username and assign it the role of **Monitor**:

The command file entry should be:

assign user "D:NT AUTHORITY\SYSTEM" to role Monitor;

Note: Any user names with special characters (other than the delimiters : and \) should be enclosed in quotes in the command file entry.

```
# symauth -sid 110 commit -f adduser.cmd

Perform an Authorization change on Symmetrix unit 000190103110 (y/[n]) ? y

PREVIEW.....Started.
PREVIEW.....Done.

COMMIT.....Started.
assign user D:NT AUTHORITY\SYSTEM to role Monitor.....Done.
COMMIT.....Done.

#
```

Note: An error gets generated in the symaudit log stating "User Authorization Failure for User D:NT AUTHORITY\SYSTEM -- 'VLOGIX' rights not present (minimum necessary role: Storage Administrator) (SID 000190100919)." This error did not impact SANscreen functionality and can be ignored.

5.7 ECC Configuration

EMC Control Center is used for storage reporting and monitoring. In order to ECC to discover and monitor the Symmetrix, it will need symacl and symauth entries to be created for the ECC Symm agent servers:

Do the following to add the ECC Symm agent server to the symacl list:

1. From the Symm agent server, get the unique ID (In this example, sangs5 is the ECC Symm agent server):

```
sangs5# symacl -unique
The unique id for this host is: 2F5802AF-5C4785C0-9A3E757A
sangs5#
```

2. From the SE server, create an accgroup called **ECC_HOST** with **BASE** and **ECC** permissions to **ALL DEVS** and add the ECC Symm agent server to the accgroup **ECC_HOST**:

The command file entry should be:

```
create accgroup ECC_HOST;
grant access=BASE,ECC to accgroup ECC_HOST for ALL DEVS;
add host accid 2F5802AF-5C4785C0-9A3E757A name sangs5 to accgroup ECC_HOST;
```

Execute the command file:

```
# symacl -sid 919 commit -f eccacl.cmd
Enter Access PIN:
Command file: (eccacl.cmd)
PREVIEW.....Started.
PREVIEW.....Done.

PREPARE.....Started.

  Creating group ECC_HOST.....Done.

  Granting access ECC to group ECC_HOST for ALL devs.....Done.

  Granting access BASE to group ECC_HOST for ALL devs.....Done.

  Adding Host access id sangs5 to group ECC_HOST.....Done.

PREPARE.....Done.

Starting COMMIT.....Done.
#
```

Do the following to add the ECC Symm agent server to the symauth list:

1. From the SE server, create a command file to create the symauth entry for the Symm agent server and assign it the role of StorageAdmin (In this case, the Symm agent server is a Solaris server with the hostname sangs5):

```
assign user H:sangs5\root to role StorageAdmin;
```

2. Execute the command file to create the symauth entry:

```
sangs7# symauth -sid 110 commit -f adduser.cmd

Perform an Authorization change on Symmetrix unit 000190103110 (y/[n]) ? y

PREVIEW.....Started.
PREVIEW.....Done.

COMMIT.....Started.
assign user H:sangs5\root to role StorageAdmin.....Done.
COMMIT.....Done.
sangs7#
```

Refer to the [ECC Solutions Guide](#) for instruction for ECC configuration.

6 Best Practices

6.1 SRDF/A

SRDF/A Best Practice is a very large subject in itself and is not covered in any detail in the present document. A separate SRDF/A Solutions Guide, and other related documents, are available on the GDSE website. These documents also cover Best Practice for SRDF/MSC and the RDF daemon, Concurrent RDF and Dynamic RDF.

The Solutions Guide covers:

- Preparation for an SRDF/A implementation
- 2-site SRDF/A configuration (with or without SRDF/MSC) and operational procedures
- 3-site Concurrent SRDF configuration and operational procedures

SRDF/A Solutions Guide	http://engineering.ti.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/05002-sg.pdf
SRDF/A Release Notes	http://engineering.ti.citigroup.net/gdse/products/platforms/symmetrix/releasenotes/05002-rn.pdf
SRDF/A Evaluation	http://engineering.ti.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/05002-e.pdf

6.2 TimeFinder/Clone

TimeFinder/Clone has its own set of Best Practice documentation and is not covered in any detail in the present document.

TimeFinder Clone Solutions Guide	http://engineering.ti.citigroup.net/gdse/products/platforms/symmetrix/releasenotes/05008-rn.pdf
TimeFinder Clone Release Notes	http://engineering.ti.citigroup.net/gdse/products/platforms/symmetrix/releasenotes/05008-rn.pdf

6.3 Volume Logix Support

The Volume Logix commands `vcmfind` and `fpath` have been replaced with `symmask`, `symmaskdb` and `symcfg` commands. All scripts utilizing Volume Logix commands must be converted to these new commands. Please refer to “**EMC Solutions Enabler Symmetrix Device Masking CLI Version 6.0 Product Guide**” for guidance on Volume Logix command conversion. Equivalent commands have also been summarized from this guide in Appendix A of the present document.

6.4 VCMDb Database Backup

The database should be backed up every day with the following command:

```
# symmaskdb -sid SymmID -file BackupFileName backup
```

The backup should be automated through the cron, and the resulting file should be sent to tape using standard backup procedures for servers.

For example, the following crontab entry would backup the vcldb of Symmetrix 1227 to a file /var/tmp/vcldb_1227_<day-of-week> at 03:00 each day. This gives the ability to roll back several days if required.

```
00 03 * * * symmaskdb -sid 1227 -file /var/tmp/vcldb_`/usr/bin/date +1227_`%A` backup
```

6.5 Heterogeneous Server Support

In instances where all FA ports are already utilized or it is otherwise not practical to dedicate a FA to one or more HP-UX hosts, heterogeneous support should be utilized to share the FA with AIX, Solaris or Windows hosts.

The HP-UX server uses Volume Set Addressing, which requires the 'V' bit to be set on the FA port. With heterogeneous masking capability, the 'V' bit will be associated with the host WWN instead of the FA port. To add a HP-UX host to a FA port that is serving other host types, use the following command for each HP-UX WWN:

```
# symmask [-sid SymmID] -wwn <WWN of the HP-UX server> \
    set heterogeneous on HP_UX -dir <FA> -p <port>
```

No changes are required to the BIN file⁶ to enable heterogeneous masking for a host. Also, there is no impact to existing hosts that are connected to that FA.

6.6 LUN Offset

The HP-UX host can only use LUNs that have octal addressing. LUNs with 8 through F in the last digit of their address cannot be seen by the HP-UX host. To make these LUNs visible to the HP-UX host, an offset can be programmed. There can be only one offset per host.

For example, if a FA port is being shared between a Solaris and HP-UX host through heterogeneous masking, and the Solaris host has been masked the LUNs with logical addressing 1 through 10 (hex), LUNs 11 (hex) to 0F (hex) can be masked to the HP-UX host by using an offset of 11 (hex). When an offset of 11 (hex) is used, the LUN addressed as 11 (hex) would appear as LUN 0 to the HP-UX host.

No changes are required to the BIN file to enable LUN offset for a host. Also, there is no impact to existing hosts that are connected to that FA.

⁶ The addressing of the LUNs behind the FA port must be compatible with the HP-UX host. The 'V' bit does not translate addressing. This issue can also be addressed in a limited way by the use of the LUN offset feature.

The process for setting the LUN Base/Offset Skip adjustment using symmask can be found in the document **“EMC Solutions Enabler Symmetrix Device Masking CLI Product Guide”**

6.7 BIN file reconfiguration with Symconfigure

Historically, the standard for BIN file changes has been to request the change through the vendor. The vendor uses the SymmWin application from the service processor to validate and implement these changes.

GDSE has certified the Symconfigure SYMCLI command, which allows for BIN file changes to be made by Citigroup personnel from a SE 5.5 or later host. This is expected to reduce the time and cost for a BIN file change. With more control over the process, Citigroup can make more frequent changes to the configuration leading to improved utilization.

Symconfigure should be used in conjunction with the meta and hyper volume standard defined in the DMX best practices document (see the references section for the location of this document) to configure the storage array. For custom sized LUNs, Symconfigure can be used to combine one or more 8GB hyper volumes into a stripe set. The command should also be used to change front end port bit settings, for configuring the SCSI 3 persistent reservation bit on a device, and assigning or removing a BCV etc.

For a complete list of certified functionality, please see [Appendix B](#).

During testing in the lab, GDSE found that symconfigure could occasionally be very slow and sometimes it can even fail. Most of the problems were found to be non-fatal, and can be recovered by re-issuing the command. The problems are related to the communication between the array and the service processor; all symconfigure commands are processed on the service processor. If a site is running into such problems, they should ask the vendor to update the service processor hardware and software to the most current version.

No examples of symconfigure usage are given in the present document. The key documentation for symconfigure which any user must familiarize themselves with is the EMC Engineering White Paper “**Using the SYMCLI Configuration manager**” which contains a very good introduction with many examples.

7 References

7.1 Key Documentation

Document	Location
EMC documentation	
EMC Solutions Enabler V6.4.2 Release Notes P/N 300-005-589	Available from EMC
EMC Solutions Enabler Symmetrix CLI Version 6.4 P/N 300-002-181	Available from EMC
EMC Solutions Enabler Symmetrix Array Contols CLI Version 6.4P/N 300-002-940	Available from EMC
EMC Solutions Enabler Symmetrix Array Management CLI Version 6.4 P/N 300-002-939	Available from EMC
EMC Solutions Enabler Version 6.4 Installation Guide P/N 300-002-289	Available from EMC
Engineering White Paper: EMC Solutions Enabler Symmetrix Device Masking CLI Product Guide	Available from EMC
Engineering White Paper: Using the SYMCLI Configuration Manager	Available from EMC
Engineering White Paper: Using SYMCLI and GNS to Propagate Group Definitions to Multiple Hosts	Available from EMC
GDSE documentation	
EMC Enginuity 5772 Release Notes	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/proposed/07023-rn.pdf
EMC Symmetrix DMX Solutions Guide	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/03038-sg.pdf
SRDF/A Solutions Guide	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/05002-sg.pdf
SRDF/A Release Notes	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/releasenotes/05002-rn.pdf
SRDF/A Evaluation	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/05002-e.pdf
TimeFinder Clone Solutions Guide	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/05008-sg.pdf

TimeFinder Clone Release Notes	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/releasenotes/05008-rn.pdf
Powerbroker Implementation for SAN	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/05006-s.pdf

7.2 Relevant Solutions Enabler 6.0 Documentation Set

The following EMC documents describe the usage of the certified components of Solutions Enabler 6.4.

EMC Solutions Enabler Documentation	
EMC Solutions Enabler Installation Guide	
EMC Solutions Enabler Symmetrix CLI Quick Reference	
EMC Solutions Enabler Symmetrix CLI Command Reference	
EMC Solutions Enabler Symmetrix Base Management CLI Product Guide	
EMC Solutions Enabler Symmetrix Device Masking CLI Product Guide	
EMC Solutions Enabler Symmetrix Access Control CLI Product Guide	
EMC Solutions Enabler Symmetrix TimeFinder Family CLI Product Guide	
EMC Solutions Enabler Symmetrix SRDF Family CLI Product Guide	
EMC Solutions Enabler Symmetrix Secure Erase CLI Product Guide	
EMC Solutions Enabler Symmetrix Change Tracker CLI Product Guide	
EMC Solutions Enabler Symmetrix Configuration Change CLI Product Guide	
Engineering White Papers	
Using SYMCLI to Obtain Symmetrix Configuration Information	
Using SYMCLI to Attach, Query, and Verify with TimeFinder Family Products	
Using SYMCLI to Set Up TimeFinder/Mirror BCV Pairs	
Using SYMCLI to Set Up TimeFinder/Mirror Multiple BCVs and Concurrent BCVs	
Using SYMCLI to Perform TimeFinder/Mirror Control Operations	
Using SYMCLI to Perform Consistent Splits with the TimeFinder Product Family	
Using SYMCLI to Perform TimeFinder/Clone Operations	
Using SYMCLI to Query and Verify with SRDF Family Products	
Using SYMCLI to Perform Control Operations with SRDF Family Products	
Using SYMCLI to Implement RDF Consistency Protection with SRDF Family Products	
Using SYMCLI to Perform Device Masking	
Using SYMCLI to Administer Symmetrix Access Control	
Using the SYMCLI Configuration Manager	
Using SYMCLI to Measure Volume Changes with Change Tracker	
Using SYMCLI and GNS to Propagate Group Definitions to Multiple Hosts	

8 Appendix A: Volume Logic Conversion

VCM command	SYMCLI command
vcmfind [-r]	symmask discover hbas [-rename]
fpath lshbawwn	symmask list hbas
fpath lshosts -d	symmask -sid list logins
fpath adddev -d [-w -u] -f -r	symmask -sid [-wwn -awwn] -dir -p add devs <r>
fpath rmdev -d [-w -u] -f -r	symmask -sid [-wwn -awwn] -dir -p remove devs <r>
fpath chgname -d -w -n	symmask -sid -wwn rename < awwn>
fpath clrwwn -d [-w -u]	symmask -sid [-wwn -awwn] delete
fpath swaphba -d [-w -u] -n	symmask -sid [-wwn -awwn] replace < awwn>
fpath chgattr -d -h	symmask -sid [-wwn -awwn] -dir -p set visibility <on off>
fpath chgattr -d -s -v	symmask -sid [-wwn -awwn] -dir -p set lockdown <on < fcid> off>
fpath chgattr -d -l -o -b	symmask -sid [-wwn -awwn] -dir -p set lunoffset <on < offset>< base> off>
fpath chgattr -d -m -c	symmask -sid [-wwn -awwn] -dir -p set heterogeneous <on < host> off>
fpath refresh -d	symmask -sid refresh
fpath lsdb -d	symmaskdb -sid list database
fpath lsbackup -o	symmaskdb -file list database
fpath lshbavols [-d -o] [-w -u]	symmaskdb -sid [-wwn -awwn] list devs
fpath initdb -d	symmaskdb -sid -file init
fpath backupdb -d	symmaskdb -sid -file backup
fpath restoredb -d	symmaskdb -sid -file restore
fpath lshostdev	sympd list -sid
fpath lssymmdev -d	symcfg list -sid -FA all -address
fpath lssymmfas -d	symcfg list -sid -FA all
fpath lsstatus -d	symcfg list -sid -v

9 Appendix B: Certified symconfigure functionality

Activity	SYMCLI command
Verify Symmetrix is ready for configuration change	symconfigure verify -sid <i>SymmlID</i>
Check for free physical disk space to configure	symconfigure list -freespace [-units CYLINDERS MB] -sid <i>SymmlID</i>
Create BCV devices.	create dev count=<# of devices>, size=<# of cylinders>, emulation=FBA, config=BCV;
Create meta BCV device	form meta from dev <metahead>, config=<metatype>, stripe_size=<stipesize [cyl]>; add dev <device range> to meta <metahead>;
Dissolve meta BCV.	dissolve meta dev <i>SymDevName</i> ;
Remove BCV devices	delete dev < <i>SymDevName</i> range>;
Create RDF device	create dev count=<# of devices>, size=<# of cylinders>, emulation=FBA, config=RDF1, remote_config=RDF2, ra_group=<RA group number>;
Enable dynamic RDF configurations.	set symmetrix dynamic_rdf = enable;
Convert static RDF to dynamic RDF	convert rdf dev <i>SymDevName</i> [: <i>SymDevName</i>] to dynamic;
Map device to FA.	map dev <i>SymDevName</i> to dir <i>director_num:port_number</i> target= <i>tid</i> , lun= <i>LunNum</i>
Unmap a device from FA.	unmap dev <i>SymDevName</i> [: <i>SymDevName</i>] from dir <i>director_num:port_number</i> ;
Change device emulation from FBA to CELERRA_FBA	set device <i>SymDevName</i> emulation= <i>EmulationType</i> ;
Change vcldb_restrict_access metric	set symmetrix vcldb_restricted_access = Enabled;
Set SRDF/A Cycle time for an RDF group	set ra group <n>, minimum_cycle_time=X;
Set SRDF/A Priority for an RDF group	set ra group <n>, session_priority=X;
Set SRDF/A Cache utilization for whole Symmetrix	set symmetrix rdfa_cache_percent=X;
Enable dynamic RDF configurations.	set symmetrix dynamic_rdf=enable;
Create meta device	form meta from dev <i>SymDevName</i> , config=MetaOption, count=member_count;
Change front end port bit settings	set port DirectorNum:PortNum HP_UX=enable;
Change SCSI 3 persistent reservation bit setting on device	set dev <i>SymDevName</i> [: <i>SymDevName</i>] attribute=[NO]device_attr;

10 Appendix C: Release Notes

Version	Changes Since Last Version
0.2	Updated the Solutions Guide for SE 6.4. • Section 3.2.1 – New symacl configuration • Section 4 – New installation instructions • Section 5.2 – SYMAPI server use is now limited for SANscreen usage only. • Section 5.4 – Role based access control using symauth • Section 5.5 – New audit logging and alerting functionality using storevntd • Section 5.6 – SE 6.4 configuration for SANscreen • Section 5.7 – SE 6.4 configuration for ECC • Section 7 – Updated references for this project.