



CATE Storage and Backup Engineering

Solutions Enabler Release 7

CSBE-11067-SG

Solutions Guide

**Document Version 1.2 for
(Solutions Enabler 7.5)**

©Citigroup Inc. 2013, 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
Draft 0.1	8-5-2011	Quang Le	Ludwig Derodel, Fabish Madathil	Peer Review
0.2	8-5-2011	Quang Le	Global Stakeholders	Release for Comments
1.0	8-19-11	Quang Le	-	Release for Production
1.1	10-14-11	Quang Le	-	Release for Production
1.2	02-21-13	G.Shimabuku	L. Derodel	Support for Point Release 7.5

CONTENTS

VERSION CONTROL.....	2
CONTENTS.....	3
LEGAL NOTICE	5
CONTACT.....	5
LATEST VERSIONS.....	5
REGIONAL REVIEWERS	5
CONFIDENTIALITY	5
1 INTRODUCTION.....	6
1.1 APPLICABLE ENVIRONMENTS.....	6
2 INSTALLATION PREPARATION.....	7
2.1 SOLUTIONS ENABLER MANAGEMENT SERVER SETUP	7
2.2 SYMMETRIX SECURITY.....	7
2.2.1 SYMACL Permissions.....	7
2.2.2 SYMACL Backup and Restore	9
2.3 LICENSING	11
3 RHEL SE SOFTWARE INSTALLATION AND CONFIGURATION	12
3.1 INSTALLING SE ON RHEL	12
3.1.1 System Requirements.....	12
3.1.2 Pre-Installation Procedure	12
3.1.3 Package Installation.....	12
3.1.4 Post-Installation Procedure.....	13
3.2 SE UNINSTALL PROCEDURE ON RHEL.....	15
3.3 SE UPGRADE PROCEDURE ON RHEL.....	15
3.3.1 Pre-Upgrade Procedure.....	15
3.3.2 Upgrade Procedure.....	16
3.4 BACKING OUT OF AN UPGRADE ON RHEL	18
4 SOLARIS SE SOFTWARE INSTALLATION AND CONFIGURATION.....	20
4.1 INSTALLING SE ON SOLARIS 10.....	20
4.1.1 System Requirements.....	20
4.1.2 Pre-Installation Procedure	20
4.1.3 Package Installation.....	20
4.1.4 Post-Installation Configuration.....	21
4.2 SE UNINSTALL PROCEDURE FOR SOLARIS.....	22
4.3 SE UPGRADE PROCEDURE FOR SOLARIS	23
4.3.1 Pre-Upgrade Procedure.....	23
4.3.2 Upgrade Procedure.....	23
4.4 BACKING OUT OF AN UPGRADE ON SOLARIS	25
5 ADDITIONAL CONFIGURATION.....	27
5.1 ENABLING THE SYMAPI SERVER.....	27
5.1.1 Introduction	27
5.1.2 SYMAPI server Configuration.....	27
5.2 ENABLING GROUP NAME SERVICES ("GNS")	28
5.2.1 Introduction	28
5.2.2 GNS User Authentication.....	29
5.2.3 Configuring GNS.....	29
5.2.4 Using GNS.....	29
5.2.5 Group Name Collisions.....	30
5.2.6 GNS Backup and Restore	31

5.2.7	GNS remote Mirroring.....	31
5.3	ENABLING SYMAUTH	32
5.3.1	To create symauth host based user entries on the array:	33
5.3.2	To create symauth domain based group entries on the array:	34
5.3.3	Backing Up and Restoring the Symauth Database	39
5.4	AUDIT LOGGING AND ALERTING	40
5.4.1	Configuring the Event Daemon (storevntd)	40
5.4.2	Configuring Symmetrix Alerting	41
5.4.3	Audit Log Reconciliation via SEMS	45
5.5	SOLUTIONS ENABLER DAEMON MANAGEMENT	46
5.6	SANSCREEN CONFIGURATION	47
5.6.1	SYMAPI Server Configuration for SANscreen.....	47
5.6.2	Symauth Configuration for SANscreen.....	49
5.7	ECC CONFIGURATION	49
6	BEST PRACTICE	51
6.1	VCMDB AND SYMACCESS DATABASE BACKUP	51
6.2	HETEROGENEOUS SERVER SUPPORT	51
6.3	BIN FILE RECONFIGURATION WITH SYMCONFIGURE	52
7	REFERENCES	53
8	APPENDIX A: FUNCTIONAL IDS.....	54

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 *CATE Storage and Backup Engineering.

Latest Versions

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

Regional Reviewers

Region	Reviewed By
Asia Pacific	No feedback
EMEA	No feedback
Japan	No feedback
Latin America/Mexico	No feedback
North America	No feedback

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 Linux 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 application within global Citigroup SAN environments. The information compiled in this document has been tested and certified by CATE Storage and Backup Engineering (CSBE).

1.1 Applicable Environments

SE is used to manage Symmetrix DMX and VMAX storage arrays. Certain functionality of SE 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.

2 Installation Preparation

2.1 Solutions Enabler Management Server Setup

An SOE RHEL +5.x host is required to install SE. The host should be connected to the SAN fabrics to which the Symmetrix storage arrays that are to be managed are connected.

For redundancy, it is recommended that two hosts be used to manage 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 4.2](#) on how the Group Name Service (GNS) is to be configured.

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.

2.2 Symmetrix Security

2.2.1 SYMACL Permissions

Symmetrix Host Access Control management (SYMACL) must be used with all Symmetrix to limit host access for 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.

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

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

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

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

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;
```

Note: There is an 8 character limit for the hostname used to name the accid.

When executing the command file, the user will be prompted to enter a PIN (the PIN is 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:

```
delete 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, ECC, and ALL rights to ALL_DEVS. Add the ECC storage agent server to the ECC_HOST accgroup.

The final symacl list should look like the following:

```
# symacl -sid 380 list -acl
```

```
Symmetrix ID: 000192601380
```

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

Note: If symauth is enabled on the storage array, only users with the Admin or SecurityAdmin role will be able to make symacl changes.

The following should be done if application hosts need access to their devices for Timefinder/SRDF control:

1. Create an accgroup for the application host.
2. Add the application host to the accgroup.
3. Create a device pool comprised of only the devices that the application host owns and needs to control.
4. Grant BCV or RDF access to the accgroup for the device pool.
5. Grant BASE access to the accgroup for ALL devices.

2.2.2 SYMACL Backup and Restore

A backup copy of the symacl database should be created before and after any symacl configurations are made.

2.2.2.1 Symacl Backup

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

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

```
symacl -sid SymmID backup -file Filename
```

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

```
# symacl -sid 380 backup -file 380symacl.bkp

# cat 380symacl.bkp
add restored accid E47FAC06-1DA1A997-45F86743 name sangs1 to accgroup AdminGrp;
add restored accid 87CBCB70-F26DB6E2-DEEF42EC name admin to accgroup AdminGrp;
add restored accid 95EBB50C-7BFD08D1-E81DC10C name sangs7 to accgroup AdminGrp;
add restored accid 6F999B76-93D21AC6-E81DC10C name sangs6 to accgroup AdminGrp;
create accgroup EMC_SP;
add restored accid C2728AE0-6E214AE3-30AEBCA4 name 380SP to accgroup EMC_SP;
create accgroup ECC_HOST;
add restored accid EF71145C-12D185EC-734B1CE0 name gdseecc3 to accgroup ECC_HOST;
grant access=ADMIN to accgroup AdminGrp for ALL devs;
grant access=ALL to accgroup AdminGrp for ALL devs;
grant access=ADMINRD to accgroup EMC_SP for ALL devs;
grant access=OPTMZR to accgroup EMC_SP for ALL devs;
grant access=BASE to accgroup EMC_SP for ALL devs;
grant access=VLOGIX to accgroup EMC_SP for ALL devs;
grant access=BASE to accgroup ECC_HOST for ALL devs;
grant access=ECC to accgroup ECC_HOST for ALL devs;
grant access=ALL to accgroup ECC_HOST for ALL devs;
```

2.2.2.2 Symacl Restore

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

To restore a backup using symacl you use the –restore option as shown below:

```
symacl -sid SymmID commit [-v|-noecho] -restore -file Filename
```

2.3 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](#) on the [CSBE website](#) 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
VProv/Symmetrix	Enables the Virtual Provisioning component

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

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

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

3 RHEL SE Software Installation and Configuration

This section covers the installation and configuration of Solutions Enabler software on the Redhat Enterprise Linux (RHEL) 5.x operating system.

3.1 Installing SE on RHEL

3.1.1 System Requirements

Minimum amount of disk space needed: 485 MB

Minimum semaphore settings:

semmni = 256
semmns = 256
semmnu = 256
semopm = 256

3.1.2 Pre-Installation Procedure

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

1. The host must be properly zoned to the Symmetrix storage array that it will manage. If this server is the initial SE server being connected to the Symmetrix, the server should be able to discover the Symmetrix array through the ACLX device once SE is installed.
2. If this is not the first SE server connected to the array and the ACLX device is unmapped from the FAs the SE server is zoned to, gatekeepers will need to be allocated to the SE server in order for the SE server to discover the array.

3.1.3 Package Installation

Refer to [Section 3.3](#) if this is an upgrade.

Steps to install SE on a RHEL server:

1. The SE package for RHEL is located in the following directory

```
$ cd /net/stealth/export1/home1.localhost/sw/Linux
```

2. Copy the SE package to SE server and expand file

```
$ cp se750XXX-Linux-i386-ni.tar.gz <target location>  
$ gunzip se750239-Linux-i386-ni.tar.gz  
$ tar -xvf se750239-Linux-i386-ni.tar
```

3. Run the following command to install the software:

```
$ ./se750XXX_install.sh -install -silent
```

4. Verify that the SE packages are at 7.X:

```
# ./se750XXX_install.sh -check

#-----
#                               EMC Installation Manager
#-----
Copyright 2010, EMC Corporation
All rights reserved.

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

Checking for Solutions Enabler Native Installer kit Installation.....

SI No RPM                               Version
-----
 1 symcli-64bit                         V7.X
 2 symcli-base                          V7.X
 3 symcli-data                          V7.X
 4 symcli-jni                           V7.X
 5 symcli-srm                           V7.X
 6 symcli-symcli                        V7.X
 7 symcli-symrecover                    V7.X
 8 symcli-thincore                      V7.X
```

3.1.4 Post-Installation Procedure

1. Set the following in the **.bash_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 to the server if that hasn't already been done.

Refer to the V-MAX Solutions Guide on the [Symmetrix Product Page](#) for recommendations on allocating gatekeepers.

5. Run the following command to build the configuration (SYMAPI) database:

```
# symcfg discover
```

6. Start the **storevntd** and **storsrvd** daemons:

```
# stordaeon start storevntd
```

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

```
# stordaeon start storsrvd
```

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

7. Run the following command to start the storevntd and storsrvd automatically after a system reboot.

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

```
# stordaeon install storsrvd -autostart
```

8. Start ECC Agents:

```
# <ECC Agent install dir>/ecclexec/eccmad start
```

9. For DMX arrays running 577X code, the VCM device is used for the initial discovery of the storage arrays by a Solutions Enabler host. Once the DMX is visible to the host, a sufficient number of gatekeepers should be assigned to the host. After the Solutions Enabler host has successfully discovered the assigned gatekeepers, the VCM device should be unmapped from all FAs on the DMX so that it will not be visible to other hosts.

The V-MAX contains a device called the ACLX device that is used for the initial discovery of the storage arrays similar to the VCM device on the DMX. By default, the ACLX device is mapped to every front-end adapter port on the V-MAX. Once hosts are zoned to the front-end ports, the ACLX device will automatically be visible to those hosts for the initial discovery of the array and will function as the communications medium until gatekeepers on the array are provisioned to the host. As a best practice, once gatekeepers have been provisioned and discovered on the Solutions Enabler management server(s), the ACLX device should be unmapped from all FAs so that it is not visible to any host. This will alleviate any attempt to use the device as a storage device and stop any system messages from flooding the logs due to an unlabeled device.

Warning: If this is the initial management server for the V-MAX storage array, ensure that gatekeepers have been assigned and discovered on the server before unmapping the ACLX device from the FAs.

Refer to the V-MAX Solutions Guide on the [Symmetrix Product Page](#) for details on unmapping the ACLX device from the FAs.

3.2 SE Uninstall Procedure on RHEL

To completely remove SE on the server, do the following:

```
# stordaeon shutdown all -immediate
# <ECC Agent install dir>/ecc/lecc/leccmad stopall
<Locate SE install shell and run with uninstall option>
# ./se75XXX_install.sh -uninstall
```

3.3 SE Upgrade Procedure on RHEL

Follow the steps in this section to upgrade to the most current certified version of SE on RHEL.

3.3.1 Pre-Upgrade Procedure

1. Run the following command to update the configuration database:

```
# symcfg discover
```

2. Create a backup of the masking database of each Symmetrix local to the SE server being upgraded:

For DMX4 models and earlier, issue the command:

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

For VMAX models, issue the command:

```
# symaccess -sid <SymmID> backup -file <BackupFilename>
```

3. As a precautionary step, export all device and composite groups to a file as a backup:

```
# symdg exportall -f <filename>
# symcg exportall -f <filename>
```

4. Record the current symacl unique ID for the server in case the upgrade process changes the unique ID of the server:

```
# symacl -unique > /var/tmp/namgdse14_uniqueID_preupgrade
```

5. Stop all Solutions Enabler daemons:

```
# stordaeon shutdown all -immediate
```

6. Stop all ECC agents:

```
# <ECC Agent install dir>/ecc/lecc/leccmad stopall
```

7. Make a backup copy of the `/var/symapi/db` directory:

```
# mkdir /var/tmp/symapi_bk
# mkdir /var/tmp/symapi_bk/db_old
# cd /var/symapi/db
# find . -print|cpio -dumpv /var/tmp/symapi_bk/db_old
```

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

```
# mkdir /var/tmp/symapi_bk/config_old
# cd /var/symapi/config
# find . -print | cpio -dumpv /var/tmp/symapi_bk/config_old
```

9. Perform a backup of the system if possible.

3.3.2 Upgrade Procedure

1. Complete the pre-upgrade procedure in the previous section.
2. The SE package for RHEL is located in the following directory

```
$ cd /net/stealth/export1/home1.localhost/sw/Linux
```

3. Copy the SE package to SE server and expand file

```
$ cp se750XXX-Linux-i386-ni.tar.gz <target location>
$ gunzip se750239-Linux-i386-ni.tar.gz
$ tar -xvf se750239-Linux-i386-ni.tar
```

4. Run the following command to install the software:

```
$ ./se750XXX_install.sh -install -silent
```

5. Verify that the Solutions Enabler packages are at version 7.X:

```
# ./se750XXX_install.sh -check

#-----
#                               EMC Installation Manager
#-----
Copyright 201X, EMC Corporation
All rights reserved.

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

Checking for Solutions Enabler Native Installer kit Installation.....

Sl No RPM                               Version
-----
 1 symcli-64bit                         V7.X
 2 symcli-base                         V7.X
 3 symcli-data                         V7.X
 4 symcli-jni                         V7.X
 5 symcli-srm                         V7.X
 6 symcli-symcli                      V7.X
 7 symcli-symrecover                  V7.X
 8 symcli-thincore                    V7.X
```

6. Run the 'symacl -unique' to check that the unique ID of the server hasn't changed from the unique ID recorded during the pre-upgrade procedure. If the unique ID has changed, use another SE server that has symacl permissions to the arrays and create a new entry for the server with its new unique ID on each array it's going to manage.

7. Rediscover the arrays:

```
# symcfg discover
```

8. Verify that prior settings in the SE configuration files have persisted after the upgrade: symapi_licenses.dat, daemon_options, netcnfg, options. If for some reason the settings did not persist, they can be restored from the backup copy.
9. If GNS was enabled, the device and composite groups on the arrays before the upgrade should still exist. If the device and composite groups were stored locally on the server and were exported before the upgrade, they can be restored by issuing the following commands:

```
# symdg importall -f <filename of file specified in the exportall command>
```

10. Start the **storevntd** and **storsrvd** daemons:

```
# stordaeon start storevntd
Waiting for daemon to start. This may take several seconds.

# stordaeon start storsrvd
Waiting for daemon to start. This may take several seconds.
```

11. Run the following command to start the storevntd and storsrvd automatically after a system reboot.

```
# stordaeomon install storevntd -autostart
# stordaeomon install storsrvd -autostart
```

12. Start ECC Agents:

```
# /export/opt/ecc/exec/eccmad start
```

3.4 Backing Out of an Upgrade on RHEL

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

1. Verify that there is a backup copy of the configuration files from the previous version which should have been created during the upgrade process in the **/backup/se7.X_rhel/symapi_bk** directories.

2. Stop all SE and ECC daemons:

```
# stordaeomon shutdown all -immediate
# <ECC Install Dir>/ecc/exec/eccmad stopall
```

3. Uninstall the current version of the SE:

```
# ./se7X_install.sh -uninstall
```

4. Install the prior version of SE that was installed on the server before the upgrade.

```
# cd /net/stealth/export1/home1.localhost/sw/Linux/se7XX_a0_linux
# ./se7X_install.sh -install -silent
```

5. If GNS was not enabled on the server, copy the backup copy of the SYMAPI database into the **/var/symapi/db**

```
# cd /backup/se7.X_rhel/symapi_bk/db_old
# find .| cpio -dumpv /var/symapi/db
```

6. Copy the old **symapi_licenses.dat** file back to the **/var/symapi/db** directory:

```
# cp /backup/se7.3_rhel/symapi_bk/config_old/symapi_licenses.dat
/var/symapi/config
```

7. Copy the backup copy of the **options** and **daemon_options** file back to the **/var/symapi/config** directory.

8. Run the following command to rebuild the configuration (SYMAPI) database:

```
# symcfg discover
```

13. Start the **storevntd** and **storsrvd** daemons:

```
sangs2# stordaemon start storevntd
```

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

```
sangs2# stordaemon start storsrvd
```

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

14. Run the following command to start the storevntd and storsrvd automatically after a system reboot.

```
sangs2# stordaemon install storevntd -autostart
```

```
sangs2# stordaemon install storsrvd -autostart
```

15. Start ECC Agents:

```
# <ECC Install Dir>/ecc/exec/eccmad start
```

4 Solaris SE Software Installation and Configuration

This section covers the steps involved in installing and configuring Solutions Enabler software on the Solaris operating system.

4.1 Installing SE on Solaris 10

4.1.1 System Requirements

Minimum amount of disk space needed: 259 MB

NOTE: Semaphore settings are obsolete as of Solaris 10.

4.1.2 Pre-Installation Procedure

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

1. The host must be properly zoned to the Symmetrix storage array that it will manage. If this server is the initial SE server being connected to the Symmetrix, the server should be able to discover the Symmetrix array through the ACLX device once SE is installed.
2. If this is not the first SE server connected to the array and the ACLX device is unmapped from the FAs the SE server is zoned to, gatekeepers will need to be allocated to the SE server in order for the SE server to discover the array.

4.1.3 Package Installation

Refer to [Section 4.3](#) if this is an upgrade.

1. Run the install script on the network share:

```
# cd /net/stealth/export1/home1.localhost/sw/PKG/se750XXX-SunOS-sparc-ni.tar.gz
# gunzip se750XXX-SunOS-sparc-ni.tar.gz
# tar -xvf se750XXX-SunOS-sparc-ni.tar
# ./se750XXX_install.sh -install -silent
```

2. Verify that the Solutions Enabler packages are at version 7.5:

```
# ./se750XXX_install.sh -check

#-----
#                               EMC Installation Manager
#-----
Copyright (c) [1997-2012] EMC Corporation. All Rights Reserved.

This software contains the intellectual property of EMC Corporation or is
licensed to EMC Corporation from third parties. Use of this software and the
intellectual property contained therein is expressly limited to the terms and
conditions of the License Agreement under which it is provided by or on behalf
of EMC.

Checking for Solutions Enabler Native Installer kit Installation.....

Sl No    Package                Version
-----
  1      SYMdse                 V7.5.0.XXX
  2      SYMse                  V7.5.0.XXX
```

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 to the server if that hasn't already been done.

Refer to the V-MAX Solutions Guide on the [Symmetrix Product Page](#) for recommendations on allocating gatekeepers.

5. Run the following command to build the configuration (SYMAPI) database:

```
# symcfg discover
```

6. Start the **storevntd** and **storsrvd** daemons:

```
sangs2# stordaeomon start storevntd
```

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

```
[/var/symapi/config]
```

```
sangs2# stordaeomon start storsrvd
```

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

```
[/var/symapi/config]
```

```
sangs2#
```

7. Run the following command to start the storevntd and storsrvd automatically after a system reboot.

```
sangs2# stordaeomon install storevntd -autostart
```

```
sangs2# stordaeomon install storsrvd -autostart
```

8. Start ECC Agents:

```
# /export/opt/ecc/exec/eccmad start
```

9. For DMX arrays running 5771 code or later, the VCM device is used for the initial discovery of the storage arrays by a Solutions Enabler host. Once the DMX is visible to the host, a sufficient number of gatekeepers should be assigned to the host. After the Solutions Enabler host has successfully discovered the assigned gatekeepers, the VCM device should be unmapped from all FAs on the DMX so that it will not be visible to other hosts.

The VMAX contains a device called the ACLX device that is used for the initial discovery of the storage arrays similar to the VCM device on the DMX. By default, the ACLX device is mapped to every front-end adapter port on the V-MAX. Once hosts are zoned to the front-end ports, the ACLX device will automatically be visible to those hosts for the initial discovery of the array and will function as the communications medium until gatekeepers on the array are provisioned to the host. As a best practice, once gatekeepers have been provisioned and discovered on the Solutions Enabler management server(s), the ACLX device should be unmapped from all FAs so that it is not visible to any host. This will alleviate any attempt to use the device as a storage device and stop any system messages from flooding the logs due to an unlabeled device.

Warning: If this is the initial management server for the V-MAX storage array, ensure that gatekeepers have been assigned and discovered on the server before unmapping the ACLX device from the FAs.

Refer to the V-MAX Solutions Guide on the [Symmetrix Product Page](#) for details on unmapping the ACLX device from the FAs.

4.2 SE Uninstall Procedure for Solaris

To completely remove SE on the server, do the following:

```
# /export/opt/ecc/exec/eccmad stopall
# ./se750XXX_install.sh -uninstall
```

4.3 SE Upgrade Procedure for Solaris

Follow the steps in this section to upgrade to the most current certified version of SE on Solaris.

4.3.1 Pre-Upgrade Procedure

1. Run the following command to update the configuration database:

```
# symcfg discover
```

2. Create a backup of the masking database of each Symmetrix local to the SE server being upgraded:

For DMX4 models and earlier, issue the command:

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

For VMAX models, issue the command:

```
# symaccess -sid <SymmID> backup -file <BackupFilename>
```

3. As a precautionary step, export all device and composite groups to a file as a backup:

```
# symdg exportall -f <filename>
# symcg exportall -f <filename>
```

4. Stop all Solutions Enabler daemons:

```
# stordaeon shutdown all -immediate
```

5. Stop all ECC agents:

```
# /export/opt/ecc/exec/eccmad stopall
```

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

```
# mkdir /var/tmp/symapi_bk
# mkdir /var/tmp/symapi_bk/db_old
# cd /var/symapi/db
# find .|cpio -pcvmud /var/tmp/symapi_bk/db_old
```

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

```
# mkdir /var/tmp/symapi_bk/config_old
# cd /var/symapi/config
# find .|cpio -pcvmud /var/tmp/symapi_bk/config_old
```

8. Perform a backup of the system if possible.

4.3.2 Upgrade Procedure

1. Complete the pre-upgrade procedure in the previous section.

2. Run the install script on the network share:

```
# cd /net/stealth/export1/home1.localhost/sw/PKG/se750XXX-SunOS-sparc-ni.tar.gz
# gunzip se750XXX-SunOS-sparc-ni.tar.gz
# tar -xvf se750XXX-SunOS-sparc-ni.tar
# ./se750XXX_install.sh -install -silent
```

3. Verify that the Solutions Enabler packages are at version 7.5:

```
# ./se750XXX_install.sh -check

#-----
#                               EMC Installation Manager
#-----
Copyright (c) [1997-2012] EMC Corporation. All Rights Reserved.

This software contains the intellectual property of EMC Corporation or is
licensed to EMC Corporation from third parties. Use of this software and the
intellectual property contained therein is expressly limited to the terms and
conditions of the License Agreement under which it is provided by or on behalf
of EMC.

Checking for Solutions Enabler Native Installer kit Installation.....

SI No   Package           Version
-----
  1     SYMdse           V7.5.0.XXX
  2     SYMse            V7.5.0.XXX
```

4. Rediscover the arrays:

```
# symcfg discover
```

5. Verify that prior settings in the SE configuration files have persisted after the upgrade: symapi_licenses.dat, daemon_options, netcnfg, options. If for some reason the settings did not persist, they can be restored from the backup copy.
6. If GNS was enabled, the device and composite groups on the arrays before the upgrade should still exist. If the device and composite groups were stored locally on the server and were exported before the upgrade, they can be restored by issuing the following commands:

```
# symdbg importall -f <filename of file specified in the exportall command>
# symcg importall -f <filename of file specified in the exportall command>
```

7. Start the **storevntd** and **storsrvd** daemons:

```
sangs2# stordaemon start storevntd
Waiting for daemon to start. This may take several seconds.

[/var/symapi/config]
sangs2# stordaemon start storsrvd
Waiting for daemon to start. This may take several seconds.

[/var/symapi/config]
sangs2#
```

8. Run the following command to start the storevntd and storsrvd automatically after a system reboot.

```
sangs2# stordaemon install storevntd -autostart
sangs2# stordaemon install storsrvd -autostart
```

9. Start ECC Agents:

```
# /export/opt/ecc/exec/eccmad start
```

4.4 Backing Out of an Upgrade on Solaris

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

1. Verify that there is a backup copy of the configuration files from the previous version which should have been created during the upgrade process in the **/var/tmp/symapi_bk/db_old** and **/var/tmp/symapi_bk/config_old** directories.
2. Stop all SE and ECC daemons:

```
# stordaemon shutdown all -immediate
# /export/opt/ecc/exec/eccmad stopall
```
3. Uninstall the current version of the SE:

```
# se750XXX_install.sh -uninstall
```
4. Install the prior version of SE that was installed on the server before the upgrade.

```
# cd /net/stealth/export1/home1.localhost/sw/PKG/se730_a0_sunos

# se7XXX_install.sh -install -silent
```
5. If GNS was not enabled on the server, copy the backup copy of the SYMAPI database into the **/var/symapi/db**

```
# cd /var/tmp/symapi_bk/db_old
# find .|cpio -pcvmud /var/symapi/db
```
6. Copy the old **symapi_licenses.dat** file back to the **/var/symapi/db** directory:

```
# cp /var/tmp/symapi_bk/config_old/symapi_licenses.dat /var/symapi/config
```
7. Copy the backup copy of the **options** and **daemon_options** file back to the **/var/symapi/config** directory.

8. Run the following command to rebuild the configuration (SYMAPI) database:

```
# symcfg discover
```

10. Start the **storevntd** and **storsrvd** daemons:

```
sangs2# stordaeomon start storevntd
Waiting for daemon to start. This may take several seconds.

[/var/symapi/config]
sangs2# stordaeomon start storsrvd
Waiting for daemon to start. This may take several seconds.

[/var/symapi/config]
sangs2#
```

11. Run the following command to start the storevntd and storsrvd automatically after a system reboot.

```
sangs2# stordaeomon install storevntd -autostart
sangs2# stordaeomon install storsrvd -autostart
```

12. Start ECC Agents:

```
# /export/opt/ecc/exec/eccmad start
```

5 Additional Configuration

5.1 Enabling the SYMAPI Server

5.1.1 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.

5.1.2 SYMAPI server Configuration

Note that a separate license is needed for SYMAPI server and is not covered by the Base license key.

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 - TCPIP - <SE server's IP address> 2707 -
```

For example:

```
SYMAPI_SERVER - TCPIP - 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 or FQDN> <username>
```

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

For example:

```
169.193.70.169 SYSTEM #SANscreen requires the SYSTEM user.
```

The SYMAPI server should now be started with:

```
# stordaemon start storsrvd
```

The following command should be executed to start the storsrvd automatically after a system reboot:

```
# stordaemon install storsrvd -autostart
```

This creates the S99emc_storsrvd startup script in the `/etc/rc3.d` directory.

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
SYMCLI_CONNECT_TYPE=REMOTE
export PATH MANPATH LD_LIBRARY_PATH SYMCLI_CONNECT SYMCLI_CONNECT_TYPE
```

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.

5.2 Enabling Group Name Services ("GNS")

5.2.1 Introduction

CSBE recommends enabling GNS. 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 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 (storrdfd).

Also with SE 6.0 or above, you can now create and restore backup (shadow) files for GNS 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.

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. Users must not modify the daemon_users file to give a non-root user rights to issue SYMCLI commands unless symauth is configured. Only root can modify the daemon_users file.

5.2.2 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 the same storage management responsibilities (and therefore need the same privileges).

5.2.3 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
<code>storgnsd:autorestart=enable</code>	Make use of the watchdog mechanism to automatically restart the daemon if it crashes.
<code>storgnsd:gns_device_poll_interval=15</code>	The interval, in seconds, at which to poll locally-attached Symmetrix arrays for group changes.
<code>storgnsd:gns_device_remote_poll_interval=60</code>	The interval, in seconds, at which to poll remotely-attached Symmetrix arrays for group changes.
<code>storgnsd:gns_rmtarr_update_interval=60</code>	Interval in seconds to use to check for group changes that need to be propagated to remote Symmetrix arrays. The default is 60 seconds.
<code>storgnsd:gns_symdiscover_interval=600</code>	The interval, in seconds, at which to check for Symmetrix configuration changes.
<code>storgnsd:gns_ppath_poll_interval=60</code>	The interval, in seconds, at which to check whether PowerPath definitions need to be updated.
<code>storgnsd:gns_shadow_file=enable</code>	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).

5.2.4 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 crashes for some reason, it will 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/MSR consistency groups as it works in companion with the RDF daemon (storrdtd). This is covered in a separate subsection.

5.2.5 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
```

5.2.6 GNS Backup and Restore

GNS group definitions are stored within the each individual Symmetrix array. 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.

The creation and restoration from backup (shadow) files maybe done manually with the following commands:

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

Note, 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.

5.2.7 GNS remote Mirroring

GDSE supports 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
```

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.

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 or Cascaded SRDF devices. It must not be used on any SE server that is used to manage a 3-Site SRDF configuration. This applies to both the production and DR site.

If remote mirroring must be enable on an SE server that is also managing a 3-Site SRDF configuration, the remote Symmetrix (remote to the SE server) in the 3-site configuration MUST be excluded from GNS management using the `gns_symavoid` option for the `storgnsd`. For example, if the remote Symmetrix on a 3-site configuration are 1380 & 217:

```
# vi daemon_options
storgnsd:gns_symavoid = 000192601380, 000194900217
```

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

5.3 Enabling symauth

GDSE currently supports two user-based access control mechanisms for Solutions Enabler:

- PowerBroker
- Symauth

One or other of these mechanisms should be implemented at your sites. This following section describes the setup of symauth.

The symauth symCLI command provides user-based authorization that assigns a user or group to a role to limit the management operations they can perform on a Symmetrix array. Solutions Enabler users 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.

Internally, Solutions Enabler represents a user/group identity as a string that comprises the user's name and authentication source. The possible encodings are:

H:HostName\UserName	A user authenticated by the local operating system.
D:DomainName\UserName	A user authenticated by a specific domain on Windows.

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.

5.3.1 To create symauth host based user entries on the array:

1. Ensure that symauth is disabled on the array:

```
# symauth -sid 110 list

S Y M M E T R I X   A U T H O R I Z A T I O N   S T A T U S

Symmetrix ID: 000190103110

Authorization Control           : Disabled

Time Enabled                   : Fri May 15 10:13:51 2009
Time Disabled                  : N/A
Time Updated                   : Mon Sep 21 20:07:26 2009

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;
```

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
#
```

On RHEL, the users with the StorageAdmin role will need to have **rwX** access to the files in the **/var/symapi/config** and **/var/symapi/db** directory.

5.3.2 To create symauth domain based group entries on the array:

User authentication can be accomplished through Windows Domain groups. This simplifies access management by assigning users to groups then managing the groups. Groups can belong to multiple SE servers, removing the redundancy of managing users for each SE server independently. The following example uses the “D” symauth nomenclature representing domain identifier of an AD group:

1. Create a command file called **assign-grp** with the following entries:

```
assign group D:NAMDEV\per_csbe_symm_admin to role StorageAdmin
```

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

```
# symauth -sid 4261 -file assign-grp commit -v -nop
```

```
PREVIEW.....Started.
  assign group D:NAMDEV\per_csbe_symm_admin to role StorageAdmin

PREVIEW.....Done.

COMMIT.....Started.
  assign group D:NAMDEV\per_csbe_symm_admin to role StorageAdmin.....Done.

COMMIT.....Done.
```

3. Verify group entry

```
# symauth -sid 4261 list -users
```

S Y M M E T R I X A U T H O R I Z A T I O N U S E R S

Symmetrix ID: 000192604261

Flags	Role	User/Group name	Component	E
--				
	Admin	User Administrator	N/A	.
	Admin	User root	N/A	.
	Admin	User smc	N/A	.
	Admin	Group L:namdev.nsrootdev.net*	N/A	.
	StorageAdmin	User H:rd-2k8r2-507srm\SYSTEM	N/A	.
	StorageAdmin	Group D:NAMDEV\per_csbe_symm_*	N/A	.
	Auditor	User H:* \storevntd	N/A	.
	Monitor	User H:GDSEEMCSMC01\SPA	N/A	.
	None	User *	N/A	.
	PerfMonitor	Group D:namdev.nsrootdev.net*	N/A	.

Legend for Flags:

(E) : N = Rule has no effect since a different rule grants greater rights.
: . = Rule is active.

```
# symauth -sid 4261 list -user -v
```

S Y M M E T R I X A U T H O R I Z A T I O N U S E R S

Symmetrix ID: 000192604261

Role name : Admin

```

User name      : Administrator
Component type :
Component name :
Flags         :

Role name      : StorageAdmin
Group name     : D:NAMDEV\per_csbe_symm_admin
Component type :
Component name :
Flags         :

```

4. Commands generated by users in an AD group are tracked by the individual user identifier:

Symaudit log:

```

Record Number      : 375635
  Records in Seq    : 1
  Offset in Seq     : 1
  Time             : 01/09/13 11:14:15
  Vendor ID        : EMC Corp
  Application ID    : SYMCONFIGURE
  Application Version : 7.5.0.7
  API Library       : SEK
  API Version       : V7.5.0.7 (Edit Level: 1604)
  Host Name        : GDSE-ECC03
  OS Name          : WinNT
  OS Revision       : 5.2.3790Se
  Client Host      :
  Process ID       : 00007152
  Task ID          : 00009664
  Function Class    : CfgChg
  Action Code       : Commit
  Text             : The local CFGCHG COMMIT operation SUCCEEDED
  Username         : D:NAMDEV\gs96899
  Activity ID      : SE92f7657591

```

Windows Event Log:

```

Event Type: Success Audit
Event Source: Security
Event Category: Object Access
Event ID: 560
Date: 1/9/2013
Time: 11:12:37 AM
User: NAMDEV\gs96899
Computer: GDSE-ECC03
Description:
Object Open:
  Object Server: Security
  Object Type: Key
  Object Name: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon
  Handle ID: 1560
  Operation ID: {0,21504116}

```

```

Process ID: 7152
Image File Name: C:\Program Files\EMC\SYMCLI\bin\symconfigure.exe
Primary User Name: gs96899
Primary Domain: NAMDEV
Primary Logon ID: (0x0,0x3E65B7)
Client User Name: -
Client Domain: -
Client Logon ID: -
Accesses: DELETE
          READ_CONTROL
          WRITE_DAC
          WRITE_OWNER
          Query key value
          Set key value
          Create sub-key
          Enumerate sub-keys
          Notify about changes to keys
          Create Link

Privileges: -
Restricted Sid Count: 0
Access Mask: 0xF003F

```

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Symevent log:

```

[fmt=symaud] [date=2013-01-09T11:12:39] [symid=000192604261] [orig=SE]
[user=D:NAMDEV\gs96899] [host=GDSE-ECC03] [actid=SE92f7657591]
[appid=SYMCONFIGURE] [aud-cls=CfgChg] [aud-act=Commit] [aud-num=375629,1/2] =
STARTING a local CFGCHG COMMIT to create new symdevs
[fmt=symaud] [date=2013-01-09T11:12:39] [symid=000192604261] [orig=SE]
[user=D:NAMDEV\gs96899] [host=GDSE-ECC03] [actid=SE92f7657591]
[appid=SYMCONFIGURE] [aud-cls=CfgChg] [aud-act=Commit] [aud-num=375630,2/2] =
create dev count=2, size=36828 cyl, emulation=FBA, config=TDEV, mvs_ssid=0;

```

To find out what the current username is for the user currently logged into the system, type the following command:

#symauth show -username

For example:

```
ql68074@sangs1#symauth show -username
```

Your current username is: H:sangs1\ql68074

Your current groupname is: H:sangs1\adm

symauth -sid 110 list -users

SYMMETRIX AUTHORIZATION USERS

Symmetrix ID: 000190103110

Role name	Username
SecurityAdmin	H:sangs7\sw54321
StorageAdmin	H:sangs7\cp12345

On RHEL, the users with the StorageAdmin role will need to have **rwX** access to the files in the **/var/symapi/config** and **/var/symapi/db** directory.

To set ACL entries for individual users, do the following:

```
# setfacl -R -m user:cp12345:rw- /var/symapi/config
# chmod 775 /var/symapi/config
# setfacl -R -m user: cp12345:rw- /var/symapi/db
# chmod 775 /var/symapi/db
```

If wanting to set the ACL entries for user groups, do the following:

```
# setfacl -R -m group:503:rwX /var/symapi/db
# getfacl /var/symapi/db
getfacl: Removing leading '/' from absolute path names
# file: db
# owner: root
# group: root
user::rwX
group::r-x
group:ql68074:rwX
mask::rwX
other::r-x
# setfacl -R -m group:503:rwX /var/symapi/config
# getfacl /var/symapi/config
getfacl: Removing leading '/' from absolute path names
# file: var/symapi/config
# owner: root
# group: root
user::rwX
group::r-x
group:ql68074:rwX
mask::rwX
other::r-x
```

Note: SE will only detect the user's primary group so when setting ACLs for groups, ensure that the ACL is set for the users' primary group.

1. The root user or a user with the proper file ACL will need to modify the **/var/symapi/config/daemon_users** file to allow the alternate users to use the daemons. For simplicity, the **<all>** entry should be used to so that this step does not have to be done for each modification to symauth. Ensure that the following line (all lower-case) is added to the daemon_users file to allow non-root users to access the Solutions Enabler daemons:

- 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
#
```

- Verify that the **Enforcement Mode** is set to **Enforce**:

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

```

S Y M M E T R I X   A U T H O R I Z A T I O N   S T A T U S

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
```

5.3.3 Backing Up and Restoring the Symauth Database

The symauth entries for each array should be backed up on a periodic basis; especially after changes are made to the entries. Use the following command to backup the symauth entries to a file on the SE management server:

```
symauth -sid <SymmID> backup -f <backup filename>
```

To restore the symauth entries from an earlier backup of the symauth database; use the following command:

symauth -sid <SymmID> commit -restore -f <backup filename>

Note: As of SE 7.2, the quotes are added around the username automatically when backing up the symauth entries.

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

5.4 Audit Logging and Alerting

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.

5.4.1 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 = syslog file           #Direct the logs and events to a local file.

storevntd:log_symmetrix_events = \
    sid=000192601380, audit, tgt=file|syslog;\ #Directs symaudit logs from the specified
Symmetrix to the local file and also send the audit event to the syslog server specified below.
    sid=000190301292, audit, tgt=file|syslog;\
    status, tgt=file;\ #Sends status messages to the file target
    events, tgt=file #Sends event messages to the file target

storevntd:log_event_file_name = symevents #Specifies the prefix of the local log file.

storevntd:log_event_syslog_host = 10.40.41.199 #IP address of the SEMS server specified
by the GSOC team.
```

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
```

```
#
```

5.4.2 Configuring Symmetrix Alerting

Citi's storage teams have the primary responsibility for responding to thin pool threshold alerts; these alerts are not sent to EMC Support Center. A plan of action should be documented for each threshold level. All other alerts are simultaneously sent to EMC via call-home mechanism and it is EMC's primary responsibility to respond. Citi storage teams should follow up with EMC to make sure they have seen the alert and they are acting on it. This will mitigate risk from call-home subsystem failure in transporting the alert to EMC Support Center. Citi problem management system can be used to document the fault and track the progress of resolution.

The storevntd daemon should be configured to record Symmetrix events to a file on the Solutions Enabler management server as specified in the previous section. Once the storevntd is configured to capture Symmetrix events, the management server will need to be configured to send events to be alerted on to Citi's Tivoli system.

The Tivoli Endpoint agent will be used to scrape the event file used by storevntd and send the alerts to the Tivoli monitoring system for alert notification to the storage support teams. Do the following to setup Tivoli monitoring and alerting:

1. If the Tivoli Endpoint agent is not yet installed on the system (the Citi package is named **CITI-Tivoli-lcfd**), it will need to be installed:
 - a. The Tivoli Endpoint agent package for Solaris is named **CITI-Tivoli-lcfd**. Do the following to install this package on Solaris:

```
# cd /net/stealth/export1/home1.localhost/sw/PKG
# pkgadd -d CITI-Tivoli-lcfd4.1.1-LCF-0020-4
```
 - b. The Tivoli Endpoint agent package for RHEL is named **CITI-Tivoli-lcfd-41120-1**. Do the following to install this package on RHEL:
 - i. Download the Tivoli Endpoint Agent (CITI-Tivoli-lcfd-41120-1.i386.rpm) from the GDS Website <https://gdsunix.nj.ssmb.com/cgi-bin/index.cgi>.
 - ii. Install the agent:

```
# rpm -ivh CITI-Tivoli-lcfd-41120-1.i386.rpm
```
2. Submit a Virtual Request to have a log file adapter created to monitor the storevntd file on the Solutions Enabler management server. Instructions for submitting the VR to the ESM group can be found at:

https://globalconsumer.collaborationtools.consumer.citigroup.net/sites/esm/Clients/Processes/Monitoring_VR.HTML

Notes on submitting the Virtual Request:

- Select **ESM Systems Monitoring – NA** as the service offering
- Select **Tivoli** for the technology
- Select **Add or Delete Logfile Adapters** for the Tivoli option
- Select **Add Logfile Adapter** for the Logfile Adapter action
- Specify the following for the Logfile Adapter. Since the text box to enter in the search strings is limited to 1000 characters, it will not be sufficient to enter in all the alerts. To get around this, enter in one request item for Warning alerts and another one for Critical alerts in the same VR ticket. For example:

User Questionnaire	ESS.Tivoli.Add Logfile Adapter
Tivoli	Add logfile adapter
Server List	sangs1.nam.nsroot.net
Full Path to Logfile	/var/symapi/log/symevents.log0 /var/symapi/log/symevents.log1

Case sensitive string to look for	Events containing the following strings (evtids listed in ranges for consecutive IDs since this box only allows 1000 chars max) should be assigned a severity level of Warning: evtid=1050-1052 evtid=1054-1056 evtid=1058-1062 evtid=1065-1066 evtid=1068-1071 evtid=1073 evtid=1075 evtid=1078-1079 evtid=1081-1083 evtid=1085-1088 evtid=1090-1101 evtid=1103-1104 evtid=1107-1108 evtid=1110 evtid=1113-1116 evtid=1127 evtid=1130-1137 evtid=1139 evtid=1143 evtid=1147 evtid=1153-1157 evtid=1200-1215 evtid=1230-1244 evtid=1280-1288 evtid=1400-1401
-----------------------------------	--

User Questionnaire	ESS.Tivoli.Add Logfile Adapter
Tivoli	Add logfile adapter
Server List	sangs1.nam.nsroot.net
Full Path to Logfile	/var/symapi/log/symevents.log0 /var/symapi/log/symevents.log1

Case sensitive string to look for	Events containing the following strings should be assigned a severity level of Critical: evtid=1053 evtid=1057 evtid=1063 evtid=1064 evtid=1067 evtid=1072 evtid=1074 evtid=1076 evtid=1077 evtid=1080 evtid=1084 evtid=1089 evtid=1102 evtid=1105 evtid=1106 evtid=1109 evtid=1111 evtid=1112 evtid=1117 evtid=1118 evtid=1119 evtid=1120 evtid=1121 evtid=1122 evtid=1123 evtid=1124 evtid=1125 evtid=1126 evtid=1128 evtid=1129 evtid=1138 evtid=1140 evtid=1141 evtid=1142 evtid=1144 evtid=1145 evtid=1146 evtid=1148 evtid=1149 evtid=1150 evtid=1151 evtid=1152 evtid=1158
-----------------------------------	--

- Once submitted the Tivoli team will contact the requestor. Email notifications will be sent out for warning alerts. Critical alerts will appear in Command Center's Tivoli TEC console and a pager notification will be sent out to the support team.

3. Start the Tivoli Endpoint agent: `/etc/Tivoli/lcf/1/setup.sh -i -g <gateway IP>`
The gateway IP should be provided by the Tivoli team once the Virtual Request is processed.

Once this has been configured, the Tivoli system should be receiving events from the Symmetrix arrays that are being managed by the Solutions Enabler server. The following is a sample of Symmetrix events as captured by the Tivoli system:

```
Citi_Hdw_San_Generic;source=APPLLOG;severity=CRITICAL;citi_probearg='1
208, [symid=000194900217] [TPDataPool=qtpool]
';hostname=sangsl;citi_profilename=CCC-CCC-CCC-EMC.D.app.prc-
logadapter;sub_source=EMC;msg='Data Pool utilization is now 100
percent. [symid=000194900217] [TPDataPool=qtpool]
';origin=10.40.42.33;END
Citi_Hdw_San_Generic;source=APPLLOG;severity=CRITICAL;citi_probearg='1
111, [symid=000194900217] ';hostname=sangsl;citi_profilename=CCC-CCC-
CCC-EMC.D.app.prc-logadapter;sub_source=EMC;msg='Save or data device
pool is full. [symid=000194900217] ';origin=10.40.42.33;END
Citi_Hdw_San_Generic;source=APPLLOG;severity=CRITICAL;citi_probearg='1
115, [symid=000194900217] ';hostname=sangsl;citi_profilename=CCC-CCC-
CCC-EMC.D.app.prc-logadapter;sub_source=EMC;msg='Save or data device
pool is almost full. [symid=000194900217] ';origin=10.40.42.33;END
Citi_Hdw_San_Generic;source=APPLLOG;severity=CRITICAL;citi_probearg='1
208, [symid=000194900217] [TPDataPool=qtpool]
';hostname=sangsl;citi_profilename=CCC-CCC-CCC-EMC.D.app.prc-
logadapter;sub_source=EMC;msg='Data Pool utilization is now 20
percent. [symid=000194900217] [TPDataPool=qtpool]
';origin=10.40.42.33;END
```

Highlighted in red (which is everything in the 'msg' field of the alert) is the notification message that will be sent to the storage support team responsible for supporting that Symmetrix.

5.4.3 Audit Log Reconciliation via SEMS

Citi's Security Event Monitoring System (SEMS) is used to centrally collect security audit events. Custom reports can then be generated from the events collected by SEMS and sent to the log review teams for reconciliation. The following steps need to be followed to integrate the Symmetrix with SEMS for audit log reconciliation:

1. storevntd needs to be configured on the SE management server to send Symmetrix syslog audit events to the SEMS server.
2. The SEMS GSOC team should be contacted to initiate the request for integrating the Symmetrix with SEMS for log reconciliation. The SE management station should be specified as the source device in the request. Use the following distribution: ***CTI Global SOC SDM**
 - a. If PowerBroker is used for user access control and audit logging, the existing log reconciliation process for PowerBroker should be followed for reconciling Symmetrix changes performed by Citi personnel. Only vendor initiated changes should be reconciled using the SEMS system for environments using PowerBroker since PowerBroker cannot track vendor changes which are initiated

on the Symmetrix Service Processor. Please note in the request to the SEMS team whether PowerBroker is being used. If Powerbroker is not being used, ensure that symauth is implemented.

- b. For environments that have implemented symauth for user access control and audit logging, all symaud events should be reported and reconciled with the exception of the events in the exclude list specified in the next step.
3. The GSOC team will then configure Arcsight to receive the Symmetrix syslog audit events and generate daily reports to the regional log review teams.

The GSOC team will apply a filter to the report to only include audit events (fmt=symaud).

Symaud events that contain the following will be excluded since they are non-change events:

- Access Denied
- Access ctrl violation

For environments still using PowerBroker, audit events showing up under the 'root' user of the SE management server should also be excluded from the report since PowerBroker has its own log review process. It is important to specify whether PowerBroker is being used in the request to the GSOC team so that they know which filter to apply to the reports for log reconciliation.

5.5 Solutions Enabler Daemon Management

The following command should be run for the storeventd, storwatchd, storrdfd, and storsrvd to ensure that these daemons are started after a reboot of the SE server:

```
# stordaeon install <daemon name> -autostart
```

If there is a monitoring system available (e.g. Tivoli ITM), it should be used to monitor the storeventd, storwatchd, storrdfd (for arrays with srdf configured), and storsrvd to ensure that these daemons are running on the SE management station. The storwatchd daemon will restart any crashed daemons automatically. If a daemon was started while the storwatchd was down, that daemon will not be monitored by the storwatchd. To verify that a daemon is being watched by storwatchd, issue the following command:

```
# stordaeon show storwatchd
```

```
Daemon State           : Running
Daemon Start Time      : Fri Sep 12 09:43:56 201X
Version                : V6.5-883 (1.0)

Total Number of Connections : 13
Number of Active Connections : 6
Total Number of Requests   : 10

Daemon Restarts Performed  : 0
Daemons Being Monitored   : storapid storgnsd storrdfd storstpdp storevntd
storsrvd
```

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 (the user SYSTEM should be used):

For example: 10.40.42.37 SYSTEM

2. Set the following in the `/var/symapi/config/daemon_options` file:

`storsrvd:security_clt_secure_lvl=NOVERIFY`

3. 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.
```

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

stordaeomon 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
```

5. The storsrvd daemon should have the following settings:

stordaeomon show storsrvd

```
Daemon State           : Running
Daemon Start Time      : Mon Apr 26 15:49:51 201X
Version                : V7.X
Auto-Restart by Watchdog : Enabled

Total Number of Connections : 1578
Number of Active Connections : 2
Total Number of Requests   : 210624

ANR0123I Show Server Details :

SYMAPI Version         : V7.X
SYMAPI Session Total/Active : 1577/2
SYMAPI Session Port    : 2707
Security Level          : SECURE
Show ANR Category       : Disabled
Show ANR Message Id     : Enabled
Enhanced Authentication : Disabled
Client Verification Level : NOVERIFY
```

#

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):

```
# symacl -unique

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

2. From the SE server, create an accgroup called **ECC_HOST** with **BASE**, **ECC**, and **ALL** 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,ALL 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.

    Granting access ALL 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.
```

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

6 Best Practice

6.1 VCMDDB and Symaccess Database Backup

For DMX storage arrays, the database should be backed up every day with the following command:

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

For V-MAX storage arrays utilizing auto-provisioning (i.e. symaccess), the database should be backed up every day with the following command:

```
# symaccess -sid 1380 -file <filename> backup -nop
```

A cron job can be created for this backup process to automate it.

6.2 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. To do this, the initiator port flag should be set at the HP-UX host initiator level.

To add a HP-UX host to a FA port that is serving other host types, use the following command for each HP-UX initiator 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.

The Heterogeneous flag is no longer supported on VMAX; however, the flag is still depicted in the symaccess output. The depiction is due to the remnant of the traditional (symmask) provisioning database. The VMAX symaccess command to turn on the Volume Set Addressing flag for HP-UX initiators is:

```
# symaccess -sid <sid> set hba_flags on V -enable -wwn <HBA wwn> dir <FA> -p <port>
```

Note: The HBA flags can only be set on an individual initiator bases in SE7.0. In SE7.1, the HBA flags will be able to be set on an initiator group level.

The syntax to set the HBA flags at an initiator group level is:

```
# symaccess -sid <SymmID> -name <GroupName> -type initiator set ig_flags <on <flag> <-enable | -disable> | off [flag]>
```

For example:

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.

```
# symaccess -sid 217 -name ig_namgdse11 -type initiator set ig_flags on V --enable
```

6.3 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 changes. With more control over the process, Citigroup can make more frequent changes to the configuration leading to improved utilization.

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

Document	Location
EMC documentation	
Solutions Enabler Installation Guide	Available from EMC
Solutions Enabler SYMCLI Command Reference HTML Help	Available from EMC
Solutions Enabler Symmetrix CLI Quick Reference	Available from EMC
Solutions Enabler Symmetrix Array Management CLI Product Guide	Available from EMC
Solutions Enabler Symmetrix Array Controls CLI Product Guide	Available from EMC
Solutions Enabler Symmetrix TimeFinder Family CLI Product Guide	Available from EMC
Solutions Enabler Symmetrix SRDF Family CLI Product Guide	Available from EMC
Solutions Enabler Symmetrix Open Replicator CLI Product Guide	Available from EMC
Solutions Enabler Symmetrix SRM CLI Product Guide	Available from EMC
Solutions Enabler Documentation Roadmap	Available from EMC
CATE documentation	
CATE Symmetrix Documentation	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/symmetrix.aspx

8 Appendix A: Functional IDs

The following table lists the functional IDs that are configured within the Symmetrix:

Application	Account	Interactive/Non-Interactive	Symauth Role	Password Change Frequency
ECC	ecc	Non-Interactive	StorageAdmin	Not required
SANscreen	sanscreen	Non-Interactive	Monitor	Not required

©Citigroup Inc. 2013, 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.