



CATE Storage and Backup Engineering

Solutions Enabler 8.0.2

CSBE-11067-SG

Solutions Guide

Document Version 1.7

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
1.3	01-17-14	G. Shimabuku	L. Derodel C.P. Williams	Support for Point Release 7.6 & LDAP/Kerberos Support
1.4	06-25-14	C.P. Williams	L. Derodel	Support for Point Release 7.6.2.8
1.5	07-15-14	C.P. Williams	-	Support for Point Release 7.6.2.25
1.6	03-24-15	Quang Le	Ludwig Derodel	Support for SE 8.0.2 and VMAX3
1.7	04-03-15	Quang Le	Global Stakeholders	Release for Comments

CONTENTS

.....	1
VERSION CONTROL.....	1
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 SYMAACL Permissions.....	7
2.2.2 SYMAACL Backup and Restore	10
2.3 LICENSING	11
3 RHEL SE SOFTWARE INSTALLATION AND CONFIGURATION	13
3.1 INSTALLING SE ON RHEL	13
3.1.1 System Requirements.....	13
3.1.2 Pre-Installation Procedure	13
3.1.3 Package Installation.....	13
3.1.4 Post-Installation Procedure.....	14
3.2 SE UNINSTALL PROCEDURE ON RHEL.....	15
3.3 SE UPGRADE PROCEDURE ON RHEL.....	15
3.3.1 Pre-Upgrade Procedure.....	16
3.3.2 Upgrade Procedure.....	16
3.4 BACKING OUT OF AN UPGRADE ON RHEL	18
4 ADDITIONAL CONFIGURATION.....	20
4.1 ENABLING THE SYMAPI SERVER.....	20
4.1.1 Introduction	20
4.1.2 SYMAPI server Configuration.....	20
4.2 ENABLING GROUP NAME SERVICES ("GNS")	21
4.2.1 Introduction	21
4.2.2 GNS User Authentication.....	22
4.2.3 Configuring GNS.....	22
4.2.4 Using GNS	22
4.2.5 Group Name Collisions.....	23
4.2.6 GNS Backup and Restore	24
4.2.7 GNS remote Mirroring.....	24
4.3 ENABLING SYMAUTH	25
4.3.1 To create symauth host based user entries on the array:	26
4.3.2 To create symauth domain based group entries on the array:	27
4.3.3 LDAP/Kerberos Linux Authentication	32
4.3.4 Backing Up and Restoring the Symauth Database	33
4.4 AUDIT LOGGING AND ALERTING.....	33
4.4.1 Configuring the Event Daemon (storevntd)	33
4.4.2 Configuring Symmetrix Alerting	34
4.4.3 Audit Log Reconciliation via SEMS	36

4.5	SOLUTIONS ENABLER DAEMON MANAGEMENT	38
4.6	ECC CONFIGURATION	39
4.7	VIPR SRM	40
4.8	HPNA SETUP	40
5	BEST PRACTICE	41
5.1	VCMDB AND SYMACCESS DATABASE BACKUP	41
5.2	HETEROGENEOUS SERVER SUPPORT	41
6	REFERENCES	42
7	APPENDIX A: FUNCTIONAL IDS.....	43
8	APPENDIX B: LDAP/KERBEROS SE GROUP ACCESS.....	44
8.1	AUTHENTICATION STRING IDENTIFICATION	44
8.2	SET-UP PROCEDURE:	44
8.3	SOLUTIONS ENABLER AUTHENTICATION USER/GROUPS ROLES	49
9	APPENDIX C: LIST OF SYMMETRIX EVENT CODES.....	50

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 Arc 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) software 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 and receive commands from 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 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 at the following URL:

https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/Symmetrix/supported_emc_symmetrix_config_matrix.pdf

2 Installation Preparation

2.1 Solutions Enabler Management Server Setup

An SOE RHEL 5.x or 6.x host is required to install SE. The SE host and Symmetrix storage arrays that are to be managed shall be connected to same the SAN fabrics.

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 limited gatekeeper resources are 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) sets up or updates the level of access control for a Symmetrix array. Before a Solutions Enabler host can issue SYMCLI commands, it requires permissions in each Symmetrix storage array's SYMACL database. All information regarding access control is stored within directly on the Symmetrix array.

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 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: 2A5B04A6-54408FCE-9B397178
#
```

Note: all host identifiers in the examples are invalid and for example only

Once EMC has enabled SYMACL, the initial symacl list should have at least the following for VMAX and earlier Symmetrix models:

```
# 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 symacl list will have the following for VMAX3:

```
# symacl -sid 973 list -acl

Symmetrix ID: 000196700973

Group Name          Pool Name          Access Type
-----
AdminGrp            ALL_DEVS           ADMIN
AdminGrp            ALL_DEVS           ALL
EmcIntrnlGrp        ALL_DEVS           ALL
EmcIntrnlGrp        ALL_DEVS           ADMINRD
EmcNasGrp            ALL_DEVS           BASE
EmcNasGrp            EmcNasPool         BASECTRL
UnknwGrp            !INPOOLS           ALL
UnknwGrp            ALL_DEVS           BASE
```

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 F963D5A6-7FECA3CD-5FE83C25 name gdsese01 to accgroup AdminGrp;
```

Note: There is an 8 character limit for the hostname used to name the acid on VMAX and earlier Symmetrix arrays. The limit is 31 characters on VMAX3.

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 973 -f addhost.cmd -v commit

Enter Access PIN:

Contents of command file: addhost.cmd
.....
add host accid F963D5A6-7FECA3CD-5FE83C25 name gdsese01 to accgroup AdminGrp;
.....

Command file: (addhost.cmd)
PREVIEW.....Started.
PREVIEW.....Done.

PREPARE.....Started.

    Adding Host access id gdsese01 to group AdminGrp.....Done.

PREPARE.....Done.

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

The accgroup UnknwGrp shall 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 SP 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 SP will need to be added to the accgroup EMC_SP. On VMAX3, the symacl entries are created for the MMCs by default and are contained in the accgroup EmcIntrnlGrp.

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 for VMAX and earlier Symmetrix models:

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

The final symacl list should look like the following for VMAX3:

symacl -sid 973 list -acl

Symmetrix ID: 000196700973

Group Name	Pool Name	Access Type
-----	-----	-----
AdminGrp	ALL_DEVS	ADMIN
AdminGrp	ALL_DEVS	ALL
EmcIntrnlGrp	ALL_DEVS	ALL
EmcIntrnlGrp	ALL_DEVS	ADMINRD
EmcNasGrp	ALL_DEVS	BASE
EmcNasGrp	EmcNasPool	BASECTRL

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 973 backup -f 0973_acl_2015-02-23.bak
```

```
$ cat 0973_acl_2015-02-23.bak
```

```
add restored accid 00FD3198-E16B13EC-DE471DA2 name nmgdse14 to accgroup AdminGrp;  
add restored accid 62514033-E9816427-DEEF42EC name admin to accgroup AdminGrp;  
add restored accid AB1723BA-B173858A-C16489F0 name gdsese01 to accgroup AdminGrp;  
grant access=ADMIN to accgroup AdminGrp for ALL devs;  
grant access=ALL to accgroup AdminGrp 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

Solutions Enabler functionality is no longer gated or protected; therefore, license keys are not needed.

Citi has an Enterprise License Agreement (ELA) covering all Symmetrix components, allowing Symmetrix feature licenses to be obtained without a purchase order. License keys are obtained through the eLicense module on EMC's PowerLink website. The license keys are added to the Symmetrix frame using the "symlmf" SYMCLI command. The following list represents a sample of the available features obtained with the license keys:

- 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/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.

License Authorization Codes (LAC) to obtain license keys: ELA30123016 and ELA30129212
--

Addition of license keys requires restarting the SYMAPI server.

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: 352 MB

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. The ACLX devices is visible on FA port 1d4 by default.
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 se8020-Linux-x86_64-ni.tar.gz <target location>
# gunzip se8020-Linux-x86_64-ni.tar.gz
# tar -xvf se8020-Linux-x86_64-ni.tar
```

3. Run the following command to install the software:

```
# ./se8020_install.sh -install -silent
```

4. Run the following to install add-on software:

```
# ./se8020_install.sh -install -silent -srm -smis
```

5. Verify that the SE packages are at 8.0.1.xxx:

```
# /opt/emc/SYMCLI/install/se8020_install.sh -check

#-----
#                               EMC Installation Manager
#-----
Copyright (c) [1997-2015] 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 RPM                                     Version
-----
 1  symcli-base                               8.0.2.2004-0.3.x86_64
 2  symcli-cert                               8.0.2.2004-0.3.x86_64
 3  symcli-data                               8.0.2.2004-0.3.x86_64
 4  symcli-smi64                              8.0.2.2004-0.3.x86_64
 5  symcli-srm                                8.0.2.2004-0.3.x86_64
 6  symcli-symcli                             8.0.2.2004-0.3.x86_64
 7  symcli-symrecover                         8.0.2.2004-0.3.x86_64
 8  symcli-thincore                           8.0.2.2004-0.3.x86_64

The below component(s) of Solutions Enabler are not installed on the host!
 1) jni - JNI Interface for EMC Solutions Enabler APIs (not mandatory)
```

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. A minimum of 6 gatekeepers should be assigned to the server if that hasn't already been done. Additional gatekeepers can be added at a later time if commands get delayed or rejected for lack of gatekeeper resources.
3. Run the following command to build the configuration (SYMAPI) database:

```
# symcfg discover
```

4. Start the stordaemons if they are not running (storapi, storgns, storrdfd, storevntd, storwatchd, storsrmd, storstdp and storsrvd):

```
# stordaeomon start <daemon name>
```

5. Run the following command to start the stordaemons automatically after a system reboot.

```
# stordaemon install storapid -autostart
# stordaemon install storgnsd -autostart
# stordaemon install storrdfd -autostart
# stordaemon install storevntd -autostart
# stordaemon install storwatchd -autostart
# stordaemon install storsrmd -autostart
# stordaemon install storstd -autostart
# stordaemon install storsrvd -autostart
```

6. Start ECC Agents:

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

7. For DMX arrays running 5773 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 VMAX/VMAX3 contains an 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 VMAX and to FA 1d4 on VMAX3. 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 Symmetrix storage array, ensure that gatekeepers have been assigned and discovered on the server before unmapping the ACLX device from the FAs.

3.2 SE Uninstall Procedure on RHEL

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

```
# stordaemon shutdown all -immediate
# <ECC Agent install dir>/ecclexec/eccmad stopall
<Locate SE install shell and run with uninstall option>
# ./se8020_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 VMAX models, issue the command:

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

For DMX4 models and earlier, issue the command:

```
# symmaskdb -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>/ecclexec/eccmad 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 se8020-Linux-x86_64-ni.tar.gz <target location>
$ gunzip se8020-Linux-x86_64-ni.tar.gz
$ tar -xvf se8020-Linux-x86_64-ni.tar
```

4. Run the following command to install the software:

```
$ ./se8020_install.sh -install -silent
```

5. Run the following command to install add-on software:

```
# ./se8020_install.sh -install -silent -srm -smis
```

6. Verify that the Solutions Enabler packages are at version 8.X:

```
# /opt/emc/SYMCLI/install/se8020_install.sh -check

#-----
#                               EMC Installation Manager
#-----
Copyright (c) [1997-2015] 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 RPM                                     Version
-----
1  symcli-base                               8.0.2.2004-0.3.x86_64
2  symcli-cert                               8.0.2.2004-0.3.x86_64
3  symcli-data                               8.0.2.2004-0.3.x86_64
4  symcli-smi64                              8.0.2.2004-0.3.x86_64
5  symcli-srm                                8.0.2.2004-0.3.x86_64
6  symcli-symcli                             8.0.2.2004-0.3.x86_64
7  symcli-symrecover                         8.0.2.2004-0.3.x86_64
8  symcli-thincore                           8.0.2.2004-0.3.x86_64

The below component(s) of Solutions Enabler are not installed on the host!
1) jni - JNI Interface for EMC Solutions Enabler APIs (not mandatory)
```

7. 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.

8. Rediscover the arrays:

```
# symcfg discover
```

9. 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.

10. 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>
```

11. Start the stordemons if they are not running (storapi, storgns, storrdfd, storevntd, storwatchd, storsrmd, storstd and storsrvd):

```
# stordemon start <daemon name>
```

12. Run the following command to start the stordemons automatically after a system reboot.

```
# stordemon install storapid -autostart
# stordemon install storgnsd -autostart
# stordemon install storrdfd -autostart
# stordemon install storevntd -autostart
# stordemon install storwatchd -autostart
# stordemon install storsrmd -autostart
# stordemon install storstd -autostart
# stordemon install storsrvd -autostart
```

13. 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/se8.X_rhel/symapi_bk directories.

2. Stop all SE and ECC daemons:

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

3. Uninstall the current version of the SE:

```
# ./se8XXX_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/SE
$ cp se76XX-Linux-i386-ni.tar.gz <target location>
$ gunzip se76XX-Linux-i386-ni.tar.gz
```

```
$ tar -xvf se76XX-Linux-i386-ni.tar
# ./se7X_install.sh -install -silent
```

5. Check to see if the accid has changed for the server after the rollback by comparing the value against the backup copy.

```
# symacl -unique
```

If the value has changed, the symacl entry will need to be removed and re-added with the new acid for this server. You will need to do this from another SE server that has access to the arrays. If there are no other SE servers, EMC will need to re-add the symacl entries.

6. 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
```

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

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

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

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

```
# symcfg discover
```

10. Start the stordaemons if they are not running (storapi, storgns, storrdfd, storevntd, storwatchd, storsrmd, storstpd and storsrvd):

```
# stordaemon start <daemon name>
```

11. Run the following command to start the stordaemons automatically after a system reboot.

```
# stordaemon install storapid -autostart
# stordaemon install storgnsd -autostart
# stordaemon install storrdfd -autostart
# stordaemon install storevntd -autostart
# stordaemon install storwatchd -autostart
# stordaemon install storsrmd -autostart
# stordaemon install storstpd -autostart
# stordaemon install storsrvd -autostart
```

12. Start ECC Agents:

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

4 Additional Configuration

4.1 Enabling the SYMAPI Server

4.1.1 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.

4.1.2 SYMAPI server Configuration

Enabling SYMAPI server functionality:

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 and edit the `/var/symapi/config/nethost` file with the host address:

```
<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:

```
# stordaeomon start storsrvd
```

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

```
# stordaeomon 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 host¹. 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)².

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 libraries³.

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

4.2 Enabling Group Name Services ("GNS")

4.2.1 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/MSC 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.

¹ CSBE does not recommend sharing hosts that are used to manage storage with other applications for security reasons.

² These are information security requirements. This will allow for tracking of storage operator activity on the server.

4.2.2 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).

4.2.3 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_symsdiscover_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).

4.2.4 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

```
# stord daemon 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 stord daemon command line utility as follows:

```
# stord daemon start storgnsd
```

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

```
# stord daemon 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 the Solutions Enabler watchdog daemon (storwatchd) will automatically try to restart the daemon. 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.

4.2.5 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
```

4.2.6 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 machine⁴.

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.

4.2.7 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
```

⁴ 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**”.

4.3 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 user ID is assigned to one role only. The following depicts the available roles:

- **Admin** - Performs all operations on a Symmetrix system, including security operations in addition to all StorageAdmin and Monitor operations.
- **SecurityAdmin** - Performs security operations on a Symmetrix system in addition to all monitor operations.
- **StorageAdmin** - Performs all management (active or control) operations on a Symmetrix system in addition to all Monitor operations. This role does not allow users to perform security operations.
- **Monitor** - Performs read-only (passive) operations on a Symmetrix system excluding the ability to read the audit log or access control definitions.

- **Auditor** - Grants the ability to view, but not modify, security settings for a Symmetrix system (including reading the audit log, symacl list, and symauth) in addition to all Monitor operations. This is the minimum role required to view the Symmetrix audit log.
- **PerfMonitor** - Performs the same operations as a monitor, with the addition of being able to set performance alerts and thresholds.

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

Authentication String	Description
H:HostName\UserName	A user authenticated by the local host operating system
D:DomainName\UserName	A user authenticated by a specific Domain on Windows
L:ServerName\UserName	A user authenticated by an LDAP Server
C:HostName\UserName	A user authenticated by the private SMC or Unisphere for VMAX 1.0 authentication service on some host
V:DomainName\UserName	A user authenticated by a Virtualization Domain

Before enabling symauth on the storage array, symauth entries should be created for users that will be managing the storage array. The symauth entries should be associated with local host authenticated users, where each user has direct access.

4.3.1 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:sangs7lsw54321 to role SecurityAdmin;
assign user H:sangs7lcp12345 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.

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

User authentication can be accomplished though 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
```

```
SYMMETRIX AUTHORIZATION USERS
```

```
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
```

```
SYMMETRIX AUTHORIZATION USERS
```

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:

```
#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:rwX /var/symapi/config
# chmod 775 /var/symapi/config
# setfacl -R -m user:cp12345:rwX /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 ACL's 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> <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:

2. 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
```

3. 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
```

4.3.3 LDAP/Kerberos Linux Authentication

LDAP/Kerberos Redhat Linux authentication utilizes group accounts in accessing the SE server. LDAP/Kerberos groups accounts simplify user management and will eventually become the default method for Linux SE server access. Configuring LDAP/Kerberos access is covered in [Section 8](#) of this document.

4.3.4 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;

4.4 Audit Logging and Alerting

The symaudit log entries can be viewed by issuing the 'symaudit' command. The Symmetrix user issuing the symaudit command must have the role of SecurityAdmin, Auditor, or Admin.

4.4.1 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 = file syslog      #Direct the logs and events to a local file and  
syslog target.  
  
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
#
```

4.4.2 Configuring Symmetrix Alerting

Symmetrix alert messages are sent to EMC Support Center by the call-home feature based in the service processor. EMC responds by initiating fixes and alerting Citi storage teams of the issue. In parallel, Citi storage teams should be seeing these alerts generated through the storage event daemon (storevntd) on the SE host and should follow up with EMC to make sure they have seen the alert and are acting on it. This redundant process mitigates the risk from a failure of the call-home subsystem transporting the alert to EMC Support Center. Citi problem management system can be used to internally 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. An event ID include list specifies the set of Symmetrix alert messages that CTI and CSBE considers critical for operation. The objective of the include list is to limit the amount of alerts deemed non-critical received by the global operations center. A complete list of event ID's is depicted in [Appendix C](#):

Do the following to setup Tivoli monitoring and alerting:

- 1) The ITM6 Redhat Linux OS Base agent need to be installed on the RHEL SE server if it hasn't already. Refer to the [RFP- Global ITM6 Linux\(i386\) OS Agent for Tivoli Monitoring](#) for instructions on installing the agent.
- 2) Submit Global Data Center Operations Automations Marketplace request to CTI DC Monitoring Services to monitor the storevntd file on the Solutions Enabler management server. Marketplace request can be found at:

https://cmp.nj.ssmb.com/marketplace/control/product/~productId=47307_253071_GLOBAL#

Notes on submitting request:

- Select **Tivoli** for the technology
- Select **Add or Delete Logfile Adapters** for the Tivoli option
- Select **Add Logfile Adapter** for the Logfile Adapter action
- Select **App Support** for Monitor Type
- Complete EMA_MonitoringSpc MS Excel questionnaire with the following parameters:

User Questionnaire	ESS.Tivoli.Add Logfile Adapter
Tivoli	Add logfile adapter
Hostname	<SE Server>
Full Path to Logfile	/var/symapi/log/symevents.log0 /var/symapi/log/symevents.log1
Case sensitive string to look for	evtid=1050 evtid=1074 evtid=1077 evtid=1080 evtid=1117 evtid=1119 evtid=1142 evtid=1144 evtid=1147 evtid=1148 evtid=1152 evtid=1201 evtid=1202 evtid=1203 evtid=1204 evtid=1208 evtid=1221

Below are the descriptions of the event IDs:

Event ID	Description
1050	Diagnostic event trace triggered.
1074	Service processor could not complete a call for service.
1077	Power system AC line interruption detected.
1080	Single SRDF link in an RDF group is not operational.
1117	Director not responding.
1119	SRDF/A session dropped: write pending limit reached. Host throttling is disabled.
1142	Power Supply A multiple fan fault.
1144	Power Supply A faulted.
1147	Power Supply B single fan fault.
1148	Power Supply B faulted.
1152	Supplemental Power Supply internal fault.
1201	Array state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1202	Director state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1203	Port state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1204	Disk state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1208	[<NAME> Pool utilization is now <NN> percent.
1221	Disk state is now [Offline Offline Spare Online Online Spare Online Degraded] (was: [Offline Offline Spare Online Online Spare Online Degraded])

- Once the request is received and processed, the Tivoli administrator will push out the Tivoli KLO Agent to the SE server to start monitoring the SE symevents files for alerting.

4.4.3 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:

- storevntd needs to be configured on the SE management server to send Symmetrix syslog audit events to the SEMS server.
- 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) and an event description containing the following:

- 1) UNMAPPING
- 2) UNMAP
- 3) MAPPING
- 4) MAP
- 5) BASE CONTROL
- 6) CREATE
- 7) ADD
- 8) DELETE
- 9) APPLY
- 10) RENAME
- 11) INITIALIZE
- 12) MODIFY
- 13) REMOVE
- 14) RWENABLE
- 15) RWDISABLE
- 16) CODELOAD
- 17) HBA_PORT_FLAGS_ENABLE
- 18) RENAME_WWN_ALIAS
- 19) CLEAR_WWN_ALIAS
- 20) HBA_PORT_FLAGS_DISABLE
- 21) HBA_PORT_FLAG_OPTION_CLEAR
- 22) REFRESH_DEVMASK_DB
- 23) ADD_DEVICES
- 24) REMOVE_DEVICES
- 25) FAST
- 26) FAST_VP
- 27) FAST_VP
- 28) DELETING
- 29) CREATING
- 30) LICENSE
- 31) DEVMASK
- 32) METADEVICE
- 33) ATTRIBUTE
- 34) BCV
- 35) CLONE

- 36) RDF
- 37) RCOPY
- 38) QoS
- 39) CFGCHG
- 40) RECOVERY

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.

4.5 Solutions Enabler Daemon Management

The following command should be run for the storevntd, storgnsd, storwatchd, storrdfd, storstpd, 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 storevntd, 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 try to automatically restart any daemon that has crashed. 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           : Mon Mar 9 16:05:13 2015
Version                     : V8.0-1953 (1.0)

Total Number of Connections  : 11
Number of Active Connections : 6
Total Number of Requests     : 9
IPC Authentication           : Passcred

Daemon Restarts Performed    : 0
Daemons Being Monitored

storapid                    : Normal Autorestart
storgnsd                    : Normal Autorestart
storrdfd                    : Normal Autorestart
storstpd                    : Normal Autorestart
storevntd                   : Normal Autorestart
storsrvd                    : Normal Autorestart
```

4.6 ECC Configuration

EMC Control Center is used for storage reporting and monitoring of Symmetrix models earlier than VMAX3 (VMAX3 will use ViPR SRM which is covered in the next section). 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.

4.7 ViPR SRM

Once certified by Citi (expected end of Q2 2015), ViPR SRM will be used for chargeback reporting for VMAX3. ViPR SRM will utilize SMI-S on the SE management server and Unisphere for VMAX to discover and report on the VMAX3 storage array. A functional ID with need to be created for ViPR SRM and assigned the symauth role of Monitor for SRM to gather the data.

4.8 HPNA Setup

Reference [GNAST Design and Standard for SAN Automated Configuration Assurance](#) for instructions for installing the HPNA client on the RHEL SE server. Once installed, a user account called 'hpnaro' is created on the OS. A symauth entry for the 'hpnaro' user will need to be created and assigned the symauth role of 'Monitor' for each Symmetrix array the SE server is managing.

5 Best Practice

5.1 VCMDB and Symaccess Database Backup

For VMAX/VMAX3 storage arrays utilizing auto-provisioning (e.g. symaccess), the database should be backed up every day with the following command:

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

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

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

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

5.2 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 file⁵ 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/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:

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

⁵ 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.

6 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

7 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
HPNA	Hpnaro	Non-Interactive	Monitor	Not required
ViPR SRM	srm_readonly	Non-Interactive	Monitor	Not required

8 Appendix B: LDAP/Kerberos SE Group Access

Solutions Enabler (SE) provides access to EMC Symmetrix arrays for provisioning, troubleshooting, monitoring and basic management. Typical user access is performed by creating a local user account on each SE server required by the user. The creation and ongoing management of individual user accounts has become time consuming with the large number of SAN production personnel, Symmetrix arrays, SE servers and SAN operational support systems deployed by Citi.

Utilizing LDAP/Kerberos accounts reduce management complexity by combining users into a group, eliminating the need for creating and managing local host accounts. The LDAP/Kerberos group can be define into a SE authentication role ([see section 8.3](#)), where all individual members within the group will have the same access profile as the group. The centralization of access management via LDAP/Kerberos coupled with role based SE symauth group functionality simplifies user administration while maintaining a sufficient level of security.

8.1 Authentication String Identification

Solutions Enabler represents a user identity as a string that comprises the user's name along with how (and where) they were originally authenticated. The possible encodings are displayed below:

Authentication String	Description
H:HostName\UserName	A user authenticated by the local host operating system
D:DomainName\UserName	A user authenticated by a specific Domain on Windows
L:ServerName\UserName	A user authenticated by an LDAP Server
C:HostName\UserName	A user authenticated by the private SMC or Unisphere for VMAX 1.0 authentication service on some host
V:DomainName\UserName	A user authenticated by a Virtualization Domain

The authentication string beginning with "H" identifies the login as authenticated by the local host operating system. As depicted in section 8.2 item 6, the LDAP/Kerberos user/group login shows authenticated by the local operating system:

```
Your current username:  H:hostname\username1
Your current groupnames: H:hostname\emc_admin
```

Indicating the LDAP/Kerberos access as local host authentication may confuse the SE administrator expecting to see and configure for the "L:ServerName\UserName" LDAP authentication string. The depiction of the "H:\HostName\UserName" host authentication string is a product of the Citi's LDAP/Kerberos configuration and does not affect group access and management. Since the access string is depicted as local host based the local host base string (H:HostName\UserName) must be used for SE role access definitions.

8.2 Set-up Procedure:

Before attempting to set-up the LDAP/Kerberos client verify if a LDAP/Kerberos configuration already exists. Use steps 1.1, 2.1 and 3.1 in following procedure to verify LDAP/Kerberos set-up. If a LDAP/Kerberos configuration exists proceed to step 4 and verify that the proper group account and users contained in with in are valid. If not, contact the LDAP/Kerberos team to create the group with the required user identifiers.

LDAP email contacts for US region is “*GT US LDAP Contacts” and “*GT US LDAP level2 support.”
Contact system administrator for LDAP contact in other regions.

1. As root user on the SE host configure the Kerberos client.

```
# /opt/KRB5clnt/bin/kjoin -K
Default Admin Server: krb5admp for Prod, krb5admu for UAT, krb5admd for Dev
Enter Admin Server: arc-ldom4.eur.nsroot.net
LDAP Business OU: usinfra
A Kerberos local host principal must be in format of "host/<FQDN>"
where FQDN is the local host's DNS fully qualified domain name.
Kerberos Principal [host/gdsese01.nam.nsroot.net]:

Configuring Kerberos client ...
Kerberos client is configured successfully in WLAB.NET.

Checking PAM configurations ...
PAM configurations are modified successfully
All operations are completed successfully.
```

The Admin Server and LDAP Business OU identifiers are examples only. The actual identifiers can be obtained from the production platform and operating system personnel.

- 1.1. Verify Kerberos and PAM configuration. The “krb5.conf” file shows default realm and Key Distribution Center have been correctly assigned :

```
# cat /etc/krb5.conf
#
# Do not edit this file manually!!!
# This file is generated by kjoin at Wed Jan  8 17:52:29 2014 from arc-ldom4
#
#
# SOE standard krb5.conf RedHat Linux
#
[libdefaults]
    default_realm = WLAB.NET
    noaddresses = true
    default_tgs_enctypes = des3-cbc-sha1 arcfour-hmac-md5
    default_tkt_enctypes = des3-cbc-sha1 arcfour-hmac-md5
    default_keytab_name = FILE:/etc/krb5/krb5.keytab

[realms]
    WLAB.NET = {
        kdc = i10-ldapkdc-vm01.nam.nsroot.net:88
        admin_server = i10-ldapkdc-vm01.nam.nsroot.net:749
        kpasswd_server = i10-ldapkdc-vm01.nam.nsroot.net:464
        master_kdc = i10-ldapkdc-vm01.nam.nsroot.net:88
    }

[domain_realm]

    i10-ldapkdc-vm01.nam.nsroot.net = WLAB.NET
    gdsese01.nam.nsroot.net = WLAB.NET
    .nsroot.net = WLAB.NET

[logging]
    default = SYSLOG:INFO:AUTH
    kdc = SYSLOG:INFO:AUTH
    admin_server = SYSLOG:INFO:AUTH
    #default = FILE:/var/krb5/kdc.log
    #kdc = FILE:/var/krb5/kdc.log
    #admin_server = FILE:/var/krb5/kadmin.log

[appdefaults]
    pam = {
```

```

        validate = true
        keytab = /etc/krb5/krb5.keytab
        banner = login
        minimum_uid = 10
        addressless = true
        use_shmem = true
        ignore_unknown_principals = true
    }
    kinit = {
        renewable = true
        forwardable = true
    }
}

```

2. Acquire keytab file

```

# /opt/KRB5clnt/bin/kjoin -T
Default Admin Server: krb5admp for Prod, krb5admu for UAT, krb5admd for Dev
Enter Admin Server: arc-ldom4.eur.nsroot.net
LDAP Business OU: usinfra
A Kerberos local host principal must be in format of "host/<FQDN>"
where FQDN is the local host's DNS fully qualified domain name.
Kerberos Principal [host/gdsese01.nam.nsroot.net]:
Enter password for host/gdsese01.nam.nsroot.net:

```

Acquiring keytab file ...
keytab is acquired successfully in WLAB.NET.

All operations are completed successfully.

Data file krb5.keytab is created

2.1. Verify existence of keytab file:

```

# file /etc/krb5/krb5.keytab
/etc/krb5/krb5.keytab: data

```

3. Set-up LDAP Client access

```

# /opt/KRB5clnt/bin/kjoin -L
Default Admin Server: krb5admp for Prod, krb5admu for UAT, krb5admd for Dev
Enter Admin Server: arc-ldom4.eur.nsroot.net
LDAP Business OU: usinfra
Host DNS FQDN [gdsese01.nam.nsroot.net]:

```

Configuring LDAP client ...
LDAP client is configured successfully in dc=wlab,dc=net

All operations are completed successfully.

3.1. Verify LDAP client set-up. The "ldap.conf" file correctly contains "wlab" domain component :

```

# cat /etc/ldap.conf
#
# Do not edit this file manually!!!
# This file is generated by kjoin at Wed Jan  8 18:00:28 2014 from arc-ldom4
#
host i10-ldapkc-vm01.nam.nsroot.net:389
uri ldap://i10-ldapkc-vm01.nam.nsroot.net:389
referrals yes
scope one
bind_timelimit 2
timelimit 20
base ou=infra,dc=wlab,dc=net
nss_base_shadow
ou=people,ou=infra,dc=wlab,dc=net?one?&(soehost=cn=gdsese01.nam.nsroot.net,ou=site_sys,dc=
wlab,dc=net)(objectclass=shadowAccount)

```

```

nss_base_passwd
ou=people,ou=infra,dc=wlab,dc=net?one?&(soehost=cn=gdse01.nam.nsroot.net,ou=site_sys,dc=
wlab,dc=net)(objectclass=posixAccount)
nss_base_group ou=group,ou=infra,dc=wlab,dc=net
nss_base_netgroup ou=netgroup,ou=infra,dc=wlab,dc=net
nss_base_services ou=services,ou=infra,dc=wlab,dc=net
nss_base_audit_user ou=people,ou=infra,dc=wlab,dc=net
nss_base_user_attr ou=people,ou=infra,dc=wlab,dc=net
nss_base_rpc ou=rpc,ou=infra,dc=wlab,dc=net
nss_base_protocols ou=protocols,ou=infra,dc=wlab,dc=net
nss_base_networks ou=networks,ou=infra,dc=wlab,dc=net
nss_base_netmasks ou=networks,ou=infra,dc=wlab,dc=net
nss_base_hosts ou=hosts,ou=infra,dc=wlab,dc=net
nss_base_ethers ou=ethers,ou=infra,dc=wlab,dc=net
nss_base_printers ou=printers,ou=infra,dc=wlab,dc=net
nss_base_auto_master automountMapName=auto_master,ou=infra,dc=wlab,dc=net
nss_base_aliases ou=aliases,ou=infra,dc=wlab,dc=net
nss_base_automount ou=infra,dc=wlab,dc=net
# Common configurations that are not defined by host profiles

ssl off
ldap_version 3
deref searching
nss_connect_policy persist
idle_timelimit 3600
#bind_policy soft
#
# nss_ldap, ver 241, introduced the following parameters
# Try all servers "tries" + "maxcontries" times without sleeping.
# If failing, sleep "sleeptime" seconds, and try all servers again.
# If failing, double sleeptime if less than "maxsleeptime".
# Otherwise, don't double sleeptime. Then, sleep and try again.
# Repeat until "tries" times with sleeps. If failing, give up.
# All try events are logged through syslog at LOG_INFO
nss_reconnect_tries 2
nss_reconnect_maxcontries 1
nss_reconnect_sleeptime 1
nss_reconnect_maxsleeptime 1

```

4. Verify LDAP/Kerberos group for SE access. In this example the “emc_admin” group contains the SE users.

```

# getent group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
news:x:13:
uucp:x:14:uucp
man:x:15:
dip:x:40:
lock:x:54:
nobody:x:99:
users:x:100:
audio:x:63:
nsd:x:28:
floppy:x:19:
vcsa:x:69:
utmp:x:22:

```

```

utempter:x:35:
pcap:x:77:
ntp:x:38:
dbus:x:81:
rpc:x:32:
mailnull:x:47:
smmsp:x:51:
rpcuser:x:29:
nfsnobody:x:4294967294:
haldaemon:x:68:
software:x:30000:
isppar:x:301349:
capacity:x:300265:
emc_admin:*:40001:st48663,cc83451,jh17802,pj99761,username1,jw53113,sh93700
users:*:100:
john_test:*:800000:jw83113
ts3310users:*:801000:ap04753user
ts3310admin:*:801001:ap04753admin

```

5. Modify the SE authentication to include the LDAP/Kerberos group. In this example LDAP/Kerberos group is added to the admin role as a local host group.

```

#symauth -sid 4261 -file assign-grp_LDAP.txt commit

Perform an Authorization change on Symmetrix unit 000192604261 (y/[n]) ? y

PREVIEW.....Started.

PREVIEW.....Done.

COMMIT.....Started.
assign group H:hostname1\emc_admin to role Admin;.....Done.

COMMIT.....Done.

```

6. Verify that the H:hostname1\emc_admin

```

# symauth -sid 4261 list -users

SYMMETRIX AUTHORIZATION USERS

Symmetrix ID: 000192604261

Role          User/Group name      Component      Flags
-----
Admin         User Administrator   N/A           .
Admin         User root           N/A           .
Admin         Group H:hostname1\emc_admin N/A           .

```

7. Log into SE with LDAP/Kerberos ID and verify user and group access profile:

```

[username1@hostname]$ symauth show -username1

Your current username:  H:hostname1\username1
Your current groupnames: H:hostname1\emc_admin

```

The user ID in the LDAP/Kerberos account cannot have a local login on the SE host.

8. Verify the proper authentication role by determining if the user is able to complete the necessary commands. The admin role provides access to all symcli commands.

```

[username1@hostname]$ symconfigure -sid 4261 verify

```

A Configuration Change Verification is in progress. Please wait...

A Configuration Change operation is in progress. Please wait...

Establishing a configuration change session.....Established.

Verifying configuration.....Verified.

Terminating the configuration change session.....Done.

The configuration verification session has succeeded.

8.3 Solutions Enabler Authentication User/Groups Roles

- **Admin** - Performs all operations on a Symmetrix system, including security operations in addition to all StorageAdmin and Monitor operations.
- **SecurityAdmin** - Performs security operations on a Symmetrix system in addition to all monitor operations.
- **StorageAdmin** - Performs all management (active or control) operations on a Symmetrix system in addition to all Monitor operations. This role does not allow users to perform security operations.
- **Monitor** - Performs read-only (passive) operations on a Symmetrix system excluding the ability to read the audit log or access control definitions.
- **Auditor** - Grants the ability to view, but not modify, security settings for a Symmetrix system (including reading the audit log, symacl list, and symauth) in addition to all Monitor operations. This is the minimum role required to view the Symmetrix audit log.
- **PerfMonitor** - Performs the same operations as a monitor, with the addition of being able to set performance alerts and thresholds.

9 Appendix C: List of Symmetrix Event Codes

Event ID	Description
1050	Diagnostic event trace triggered.
1051	Remote (SRDF) diagnostic event trace triggered.
1052	Too many suspend/halt chains encountered switching to Adaptive Copy Write Pending Mode.
1053	Memory bank(s) automatically disabled due to cache error.
1054	Hot Spare invoked against a disk.
1055	M2 mirror resynchronizing with its M1 mirror.
1056	M1 mirror resynchronizing with its M2 mirror.
1057	Disk director not responding.
1058	Data migration completed on all migration devices.
1059	Device resynchronization process started.
1060	Hot Spare invoked against a remote R2 mirror disk.
1061	SIM message initiated to a remote SRDF attached array.
1062	SRDF error occurred.
1063	Fibre Channel front-end has failed or is inoperable.
1064	No SRDF links in an RDF group are operational.
1065	All SRDF links in an RDF group are operational.
1066	Bus Arbiter problem.
1067	Internal temperature too high.
1068	Alarm signal was set, but no alarm found.
1069	Power subsystem alarm or fault has occurred.
1070	Device mirror not ready.
1071	Device mirror write disabled.
1072	SRDF R2 device not ready.
1073	Service processor down or not communicating with array.
1074	Service processor could not complete a call for service.
1075	Abnormal DC voltage (perhaps 12 Volts) situation exists.
1076	Power subsystem environmental sense cable missing.
1077	Power system AC line interruption detected.
1078	Battery system not fully charged.
1079	Latched alarms discovered for the power subsystem.
1080	Single SRDF link in an RDF group is not operational.
1081	Single SRDF link in an RDF group is now operational.
1082	Service processor successfully completed a call for service.
1083	Subsystem unable to set a shared register.
1084	Disabled memory bank error reported to a host.
1085	Validity problem detected during environmental test.
1086	Environmental testing enabled in diagnostic mode.

1087	Communication board data does not match expected value.
1088	Communication board information mismatch.
1089	Failure detected during thermal test.
1090	Power-on-Time inconsistencies detected.
1091	No records found for the last service processor connection time.
1092	Service processor communicating via a serial line.
1093	Remote session to the service processor connected.
1094	Remote session to the service processor denied access.
1095	Remote session to the service processor disconnected.
1096	Service processor detected excessive memory usage.
1097	Battery test detected a failure.
1098	Service processor could not communicate with a director.
1099	Service processor could not query a director.
1100	Service processor is communicating via local director.
1101	Service processor unable to read an environmental sensor.
1102	Service processor detected a failed or unrecognized communications card.
1103	Service processor found environmental readings to be out of limits.
1104	Service processor disk is full.
1105	Service processor detected a smoke detector malfunction.
1106	Service processor detected a smoke detector alert.
1107	Service processor triggered a call home for service.
1108	Database Double Checksum event triggered.
1109	RDF CG trip event triggered.
1110	Service processor successfully rebooted.
1111	SAVE device pool is full.
1112	SRDF/A session inactive.
1113	SRDF/A session active.
1114	Volume (device) not ready.
1115	SAVE device pool is almost full.
1116	Active device in SAVE device pool not ready.
1117	Director not responding.
1118	Timeout writing to an R2 device; writes pending limit reached.
1119	SRDF/A session dropped: write pending limit reached. Host throttling is disabled.
1120	SRDF/A session dropped: write pending limit reached. Host throttling is enabled.
1121	SRDF/A session dropped: device not ready.Tolerance mode is off.
1122	SRDF/A session dropped: device not ready through consistency group.
1123	SRDF/A session dropped: no SRDF links operational.
1124	SRDF/A session dropped: timeout in MSC mode.
1125	SRDF/A session dropped: timeout on Host Adapter.
1126	SRDF/A session dropped: timeout on RA.

1127	Double Checksum (generic) event triggered.
1128	One of the Power Zones is down - shutdown will occur in 20 hours.
1129	One of the Power Zones is down - shutdown will occur in five hours.
1130	SRDF/A session drop requested [host software initiated].
1131	SRDF/A session drop at cycle boundary requested [host software initiated].
1132	SRDF/A session transition out of Asynchronous mode requested [host software initiated].
1133	SRDF/A session transition from Asynchronous to Synchronous mode requested [host software initiated].
1134	SRDF/A session drop requested.
1135	SRDF/A session drop at cycle boundary requested.
1136	SRDF/A session transition out of Asynchronous mode requested.
1137	SRDF/A session transition from Asynchronous to Synchronous mode requested.
1138	SRDF/A session entering transmit idle state.
1139	SRDF/A session recovered from transmit idle state.
1140	SRDF/A session dropped, transmit idle state timeout.
1141	SRDF/A session dropped, no online RAs
1142	Power Supply A multiple fan fault.
1143	Power Supply A single fan fault.
1144	Power Supply A faulted.
1145	Power Supply A shutdown.
1146	Power Supply B multiple fan fault.
1147	Power Supply B single fan fault.
1148	Power Supply B faulted.
1149	Power Supply B shutdown.
1150	Link Card Controller A temperature high.
1151	Link Card Controller B temperature high.
1152	Supplemental Power Supply internal fault.
1153	Supplemental Power Supply battery end of line.
1154	Supplemental Power Supply low input AC Voltage.
1155	Entries are being written to the audit log at an unusually high rate.
1156	Audit log has lost its redundancy due to SFS mirror being offline.
1157	Audit log entries have been overwritten in an unusually short period of time.
1158	SRDF/A session dropped, write pending limit reached on a cache partition.
1159	There has been no SRDF/A cycle switching within the past hour.
1160	The job flow control setting has changed on RDF group.
1200	Device state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1201	Array state has changed to [Not Present Unknown Online Write Disabled Offline Failed].

1202	Director state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1203	Port state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1204	Disk state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1205	Device configuration has changed.
1206	[Snap SAVEdev SRDF/A Delta Set Extension] pool state has changed to [Not Present Unknown Online Write Disabled Offline Failed].
1207	[Snap SAVEdev SRDF/A Delta Set Extension] pool configuration has changed.
1208	<NAME> Pool utilization is now <NN> percent.
1209	Symmetrix external lock has been [released acquired].
1210	Disk hot spare [is no longer invoked against a failed disk has been invoked against a failed disk].
1211	Number of available disk hot spares is N.
1212	Virtual device is now N percent allocated.
1213	Virtual device is now N percent used.
1214	Director configuration has changed.
1215	Port configuration has changed.
1221	Disk state is now [Offline Offline Spare Online Online Spare Online Degraded] (was: [Offline Offline Spare Online Online Spare Online Degraded])
1230	Array configuration has changed.
1231	Device Masking database has changed.
1232	Access Control definitions have changed.
1233	Dynamic RDF operation performed on device.
1234	Snap session created, activated or deleted.
1235	BCV device pairing has changed.
1236	HPUX device identifier has changed.
1237	Device name has changed.
1238	Device nice name has changed.
1239	OpenVMS device identifier has changed.
1240	Device reservations data has changed.
1241	Time since last SRDF/A cycle switch exceeds minimum cycle time by n seconds.
1242	SRDF/A cycles now using nn percent of the cache available for it.
1243	Write pending data is now using nn percent of the cache.
1244	Component state has changed to {Not Present Unknown Online Write Disabled Offline Failed}.
1245	Component state has changed to Online Online [Degraded] Offline Unknown

1246	Disk Group has changed. or Disk Group has been deleted. or Disk Group has been created.
1247	Disk has spare coverage. or Disk no longer has spare coverage.
1248	The spare capacity percentage for diskgroup on engine %d has changed
1249	Disk has spare coverage. or Disk no longer has spare coverage.
1280	Cache partitioning configuration has changed.
1281	Dynamic mapping configuration for a device has changed.
1282	Meta configuration for a device has changed.
1283	Initiator group has changed.
1284	Storage group has changed.
1285	Director Port group has changed.
1286	Masking view has changed.
1287	Feature registration database has changed.
1288	Application registration database has changed.
1289	optimizer,FAST tiers have changed
1290	optimizer,FAST policies have changed
1291	optimizer,FAST associations have changed
1292	optimizer,Optimizer/FAST time windows have changed
1293	optimizer,Optimizer/FAST control parameters have changed
1294	Storage group configuration has changed.
1295	Initiator group configuration has changed.
1296	Port group configuration has changed.
1297	Masking view configuration has changed.
1298	Storage group scope has changed.
1299	Initiator group scope has changed.
1300	Masking view scope has changed
1301	Indicates that a change has been made to the FAST (Fully Automated Storage Tiering) control parameters on the Symmetrix array.
1400	User authorization rules have changed.
1401	Audit log is at nn percent of capacity (before wrapping).
1402	Security Alert from Audit Log.
1403	Security Failure Alert from Audit Log.
1404	Message from Audit Log.
1500	Optimizer Swap activity (from Audit Log).
1501	Optimizer Move activity (from Audit Log).

1502	Optimizer configuration change (from Audit Log).
1503	FAST Controller Swap activity (from Audit Log).
1504	FAST Controller Move activity (from Audit Log).
1505	FAST Controller configuration change (from Audit Log).
1506	Optimizer Rollback activity (from Audit Log).
1507	User approval is required for a Config Change plan generated by the Optimizer/FAST Controller.
1508	The FAST (DP or VP) controller has switched to a different state.
1509	The Optimizer has switched to a different mode.
1510	%s FAST policy allocated capacity is now %u percent.
1511	FAST Tier (%s) performance changed
1512	The allocation for SRP has changed.
1513	The Snapshot capacity for SRP has changed to [0..100] percent."
1601	GNS is now using [0..100] percent of the available group space
1602	GNS is now using [0..100] percent of the available group directory entries.
1650	The polling cycle is complete.