EMC® VMAX® All Flash and VMAX3™ Family

Security Configuration Guide

REVISION 11

EMC²

Published May 2017

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

FIGURES

TABLES

Preface

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC representative if a product does not function properly or does not function as described in this document.

Note

This document was accurate at publication time. New versions of this document might be released on EMC Online Support (https://support.emc.com). Check to ensure that you are using the latest version of this document.

Purpose

This guide helps you to securely deploy and maintain VMAX3 and VMAX All Flash arrays, including Solutions Enabler, Unisphere® for VMAX®, SMI-S, and vApp Manager. This guide provides references to VNX® documentation to help you securely deploy embedded NAS.

Audience

This document is intended for security administrators and operators that need to understand and maintain VMAX3 and VMAX All Flash security.

Related documentation

The following EMC publications provide additional information related to managing security for your software and storage system configuration. For a comprehensive list of documentation, see the *EMC VMAX3 Family Product Guide for VMAX 100K, VMAX 200K, VMAX 400K with HYPERMAX OS* or the *EMC VMAX All Flash Product Guide for VMAX 250F, 450F, 850F, 950F with HYPERMAX OS* .

EMC VMAX All Flash Site Planning Guide for VMAX 250F, 450F, 850F, 950F with HYPERMAX OS

Provides planning information regarding the purchase and installation of a VMAX 250F, 450F, 850F, 950F with HYPERMAX OS.

EMC VMAX3 Family Site Planning Guide for VMAX 100K, VMAX 200K, VMAX 400K with HYPERMAX OS

Provides planning information regarding the purchase and installation of a VMAX3 Family 100K, 200K, 400K.

EMC Solutions Enabler, VSS Provider, and SMI-S Provider Release Notes

Describes new features and any known limitations.

EMC Solutions Enabler Installation and Configuration Guide

Provides host-specific installation instructions.

EMC Solutions Enabler CLI Reference Guide

Documents the SYMCLI commands, daemons, error codes and option file parameters provided with the Solutions Enabler man pages.

EMC Solutions Enabler Array Controls and Management for HYPERMAX OS CLI User Guide

Describes how to configure array control, management, and migration operations using SYMCLI commands for arrays running HYPERMAX OS.

EMC Solutions Enabler Array Controls and Management CLI User Guide

Describes how to configure array control, management, and migration operations using SYMCLI commands.

EMC Solutions Enabler SRDF Family CLI User Guide

Describes how to configure and manage SRDF environments using SYMCLI commands.

SRDF Interfamily Connectivity Information

Defines the versions of HYPERMAX OS and Enginuity that can make up valid SRDF replication and SRDF/Metro configurations, and can participate in Non-Disruptive Migration (NDM).

EMC Solutions Enabler TimeFinder SnapVX for HYPERMAX OS CLI User Guide

Describes how to configure and manage TimeFinder SnapVX environments using SYMCLI commands.

EMC Solutions Enabler SRM CLI User Guide

Provides Storage Resource Management (SRM) information related to various data objects and data handling facilities.

EMC Common Object Manager (ECOM) Toolkit Deployment and Configuration Guide

Describes how to securely deploy the EMC Common Object Manager (ECOM).

EMC Unisphere for VMAX Release Notes

Describes new features and any known limitations for Unisphere for VMAX .

EMC Unisphere for VMAX Installation Guide

Provides installation instructions for Unisphere for VMAX.

EMC Unisphere for VMAX Online Help

Describes the Unisphere for VMAX concepts and functions.

EMC VMAX VASA Provider Release Notes

Describes new features and any known limitations for VASA Provider.

EMC vApp Manager for Unisphere for VMAX Online Help

Describes the vApp Manager for Unisphere for VMAX concepts and functions.

EMC vApp Manager for Solutions Enabler Online Help

Describes the vApp Manager for Solutions Enabler concepts and functions.

EMC vApp Manager for eManagement Online Help

Describes the vApp Manager for embedded Management concepts and functions.

EMC vApp Manager for VASA Provider Online Help

Describes the vApp Manager for VASA Provider concepts and functions.

EMC VMAX Embedded NAS Release Notes

Describes the new features and identify any known functionality restrictions and performance issues that may exist in the current version.

EMC VMAX Embedded NAS Quick Start Guide

Describes how to configure eNAS on a VMAX3 or VMAX All Flash storage system.

EMC Unisphere for VNX Online Help

Describes how to configure embedded NAS.

EMC VNX Series Security Configuration Guide for VNX

Describes security settings and configuration for embedded NAS.

EMC VNX Series Command Line Interface Reference for File

Describes CLI commands to manage access control, certificates, LDAP configuration, and other security-related activities for embedded NAS.

EMC Mainframe Enablers Installation and Customization Guide

Describes how to install and configure Mainframe Enablers software.

EMC Mainframe Enablers Release Notes

Describes new features and any known limitations.

Special notice conventions used in this document

EMC uses the following conventions for special notices:

DANGER

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Addresses practices not related to personal injury.

Note

Presents information that is important, but not hazard-related.

Typographical conventions

EMC uses the following type style conventions in this document:

Table 1 Typographical conventions used in this content

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications referenced in text

Table 1 Typographical conventions used in this content (continued)

`Monospace`	Used for: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
`Monospace italic`	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information

EMC technical support, documentation, release notes, software updates, or information about EMC products can be obtained on the https://support.emc.com site (registration required).

Technical support

To open a service request through the https://support.emc.com site, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Reporting security vulnerabilities

EMC takes reports of potential vulnerabilities in our products very seriously. For the latest on how to report a security issue to EMC, please see the EMC Product Security Response Center at http://www.emc.com/products/security/product-security-response-center.htm.

Your comments

Your suggestions help us improve the accuracy, organization, and overall quality of the documentation. Send your comments and feedback to:
VMAXContentFeedback@emc.com

Revision history

The following table lists the revision history of this document.

Table 2 Revision history

Revision	Description and/or change
11	Added new content on D@RE. Added section on replication and secure snaps.
10	Combined individual VMAX3 Family and VMAX All Flash Security Configuration Guides into a single guide to cover both product lines. Added new content for mainframe systems.
09	Updated all security controls maps. Removed procedural information from Solutions Enabler section. Procedures now reside in the *EMC Solutions Enabler Array Controls and Management for HYPERMAX OS CLI User Guide* and the *EMC Solutions Enabler Installation and Configuration Guide*.
08	Added content on restricting vApp client access to a single domain.
07	New content describing VASA Provider. Changed/updated content: • Solutions Enabler 8.2 network encryption supports OpenSSL 1.0.1q
06	Minor updates and fixed typos.
05	New content: • Added “Configure Certificate Revocation List for X.509 Certificate-based Authentication” • Embedded NAS chapter renamed to Container applications. New content added on access IDs and embedded management. Changed/updated content: • Solutions Enabler 8.1 network encryption supports OpenSSL 1.0.1p • “manager_server_cert commands syntax” updated to support certificates with keysize of 3072 • “Resetting the host system SSVs” updated to clarify that SMAS service must be running to reset SSVs
04	New content describing Data at Rest Encryption (D@RE). Changed/updated content: • Updated steps to manage Unisphere for VMAX certificates • Updated steps to manage vApp persistent files
03	New content describing security procedures for SMI-S and an introduction to Embedded NAS.
02	New title: *EMC VMAX Family Security Configuration Guide*. New content describing security procedures for vApp Manager.

Table 2 Revision history (continued)

Revision	Description and/or change
	Updates for Solutions Enabler 8.0 and Unisphere for VMAX 1.6: • Multiple authorization roles • Managing the Lockbox
01	*EMC Symmetrix Security Configuration Guide* for Solutions Enabler 7.6 and Unisphere for VMAX 1.5.

CHAPTER 1

Overview

This chapter includes the following topics:

System Overview

EMC storage arrays running HYPERMAX OS provide industry-leading, information-centric security to secure people, infrastructure and data. You can authenticate, authorize and audit activities across systems and devices.

Points of access

There are two points of access to an array running HYPERMAX OS: Direct access to the physical system or through array control management. You can manage an array through host management or from embedded management (eManagement) directly on the array.

The following points of access must be secured in a HYPERMAX OS system:

- Physical: Physical security encompasses limiting who has access to the datacenter and array hardware. It also includes monitoring port access under normal and service operations.
- Host: Traditional host-based management allows you to manage multiple arrays from a single management interface. The host can be a physical server or a virtual machine. Host management applications include:
  - Solutions Enabler: Solutions Enabler provides a comprehensive command line interface, called SYMCLI, to manage your storage environment. SYMCLI commands are invoked from the host, either interactively on the command line, or using scripts.
  - Unisphere for VMAX: Unisphere provides a web-based application that allows you to quickly and easily provision, manage, and monitor arrays.
  - SMI-S Provider: SMI-S Provider supports the SNIA Storage Management Initiative (SMI), an ANSI standard for storage management. This initiative has developed a standard management interface that resulted in a comprehensive specification (SMI-Specification or SMI-S). SMI-S defines the open storage management interface, to enable the interoperability of storage management technologies from multiple vendors. These technologies are used to monitor and control storage resources in multivendor or SAN topologies.
    Solutions Enabler provides the interface between the SMI and the arrays. The Solutions Enabler components required for SMI-S Provider operations are included as part of the SMI-S Provider installation.
  - Mainframe Enabler: EMC Mainframe Enablers allow you to monitor and manage an array running HYPERMAX OS.
- Embedded: Embedded applications are virtual machines that provide embedded functionality on the array. Virtual hardware resources are used by the embedded applications, including:
  - Virtual hardware needed to run the software and embedded application (processor, memory, PCI devices, virtual power management)
  - Virtual FA ports (on the director where the container is installed)
  - Access to necessary drives (boot, root, swap, persist, shared)

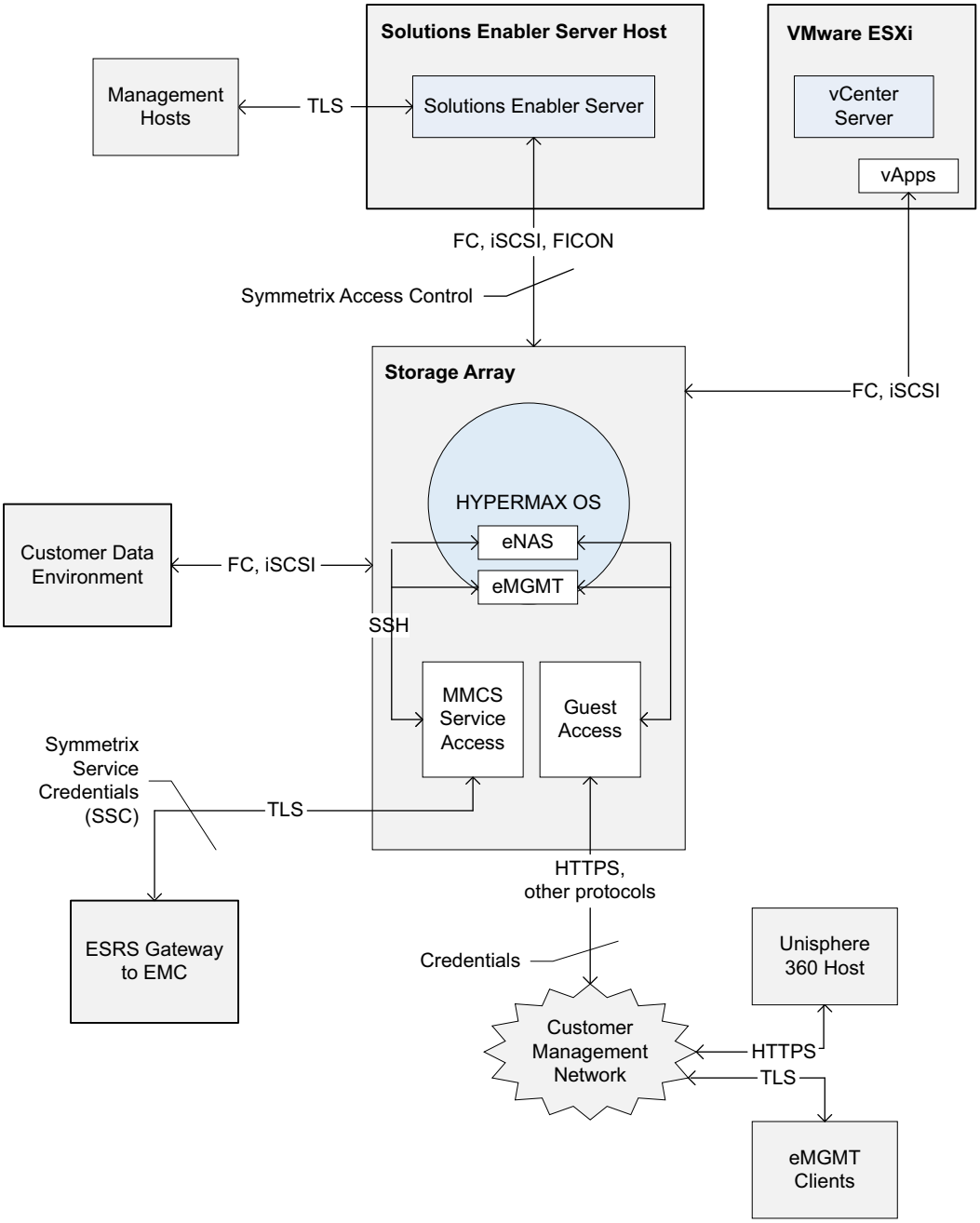
  Two embedded applications are available: Embedded NAS (eNAS) and embedded management (eManagement). eNAS enables consolidated block and file storage without the expense and complexity of gateway hardware. eManagement embeds

management software (Solutions Enabler, Unisphere for VMAX and SMI-S) on the array, enabling you to manage the array without software installed on a host.

Enbedded applications are installed at the factory. No additional security procedures are required.

Security controls map

Figure 1 System components for VMAX All Flash and VMAX3 storage arrays



CHAPTER 2

Physical Security

This chapter describes physical security controls that you should put in place to ensure a secure environment. Topics include:

Physical security controls

You are responsible for providing a secure physical environment for an array running HYPERMAX OS. A secure environment includes basic measures such as providing sufficient doors and locks, permitting only authorized and monitored physical access to the system, providing a reliable power source, and following standard cabling best practices.

Port security

A storage array includes a number of physical ports. You should ensure that only authorized personnel have access to the ports and that they are used for their intended purpose.

CHAPTER 3

Solutions Enabler

Solutions Enabler provides a comprehensive command line interface (SYMCLI) to manage your storage environment.

Solutions Enabler is available as a host-based component, as part of embedded management, or as a virtual application. This chapter addresses the host-based component.

SYMCLI commands are invoked from the host, either interactively on the command line, or using scripts.

Solutions Enabler 8.0 or greater is required to discover storage arrays running HYPERMAX OS.

This chapter contains the following topics:

Solutions Enabler checklist

The following checklist summarizes the security-related tasks you should perform to improve the security of your deployment.

Table 3 Solutions Enabler security configuration checklist

Purpose of activity	Task
Host-based access control	
Restrict which hosts may access specific functionality.	Configure SYMAPI options. Use the symacl command to generate unique ID for each management host.
Restrict actions hosts can execute.	Configure SYMAPI options and use the `symacl` command to enable use of Alternate Access IDs. Define Access Control Groups, Pools, and Hosts to control what actions management hosts can execute.
Restrict which hosts and users may perform management operations.	Use access control or user authorization to restrict hosts.
Client/server security settings	
Reduce local attachments between hosts and storage arrays.	Use Solutions Enabler in client/server mode to a `storsrvd` running on a remote host locally attached to the storage.
Protect access to Solutions Enabler resources through firewalls and NATs.	If a firewall or NAT router is used to protect network resources, you may need to: • Configure the network resources to allow access to specific ports. • Modify related settings in daemon_options.
Certificate files	
Require client authentication by the server using client certificates.	Set security_clt_secure_lvl=MUSTVERIFY in the daemon_options file.
Strengthen your authentication by using custom certificates.	Replace SYMAPI-generated security certificates with more secure customer-supplied certificates.
On client hosts	
Control ports used by the client-side event daemon (`storevntd`).	Modify the port on which the client-side `storevntd` listens.
Specify the host (HostName) and port (NNNN) on which the server daemon is listening.	For SYMCLI users, modify the `netcnfg` file with the hostnames or IP addresses of your servers.
On server hosts	

Table 3 Solutions Enabler security configuration checklist (continued)

Purpose of activity	Task
Control the port used by the server daemon (`storsrvd`).	Modify the port on which `storsrvd` listens (resolve port conflicts).
Control startup of the server daemon (`storsrvd`).	Use the `stordaemon install` command to configure `storsrvd` be started automatically at system boot.
Limit the set of client hosts from which the server will accept connections.	Configure the following: • *<SYMAPI_HOME>*`/config/nethost` file • The following entries in the *<SYMAPI_HOME>*`/config/daemon_options` file: ▪ `max_sessions` ▪ `max_sessions_per_host` ▪ `max_sessions_per_user`
Restrict the functionality that the `storsrvd` daemon is allowed to perform on behalf of remote client hosts.	Edit the following entries in the *<SYMAPI_HOME>*`/config/options` file: • `SYMAPI_ACC_ADMIN_VIA_SERVER` • `SYMAPI_ACC_DISPLAY_VIA_SERVER` • `SYMAPI_ALLOW_SCRIPTS_VIA_SERVER` • `SYMAPI_CTRL_VIA_SERVER`
Securing directories	
Protect the SYMAPI directory and its contents so that only appropriate administrators have write access.	Protect the `<SYMAPI_HOME>/config` directory.
Protect the `<SYMAPI_HOME>/db` directory to grant non-root users access.	Configure daemon_users to authorize non-root users to use daemons. Run SYMCLI commands as a non-root or non-Administrator user. Limit write access privileges to the `<SYMAPI_HOME>/db` directory to authorized users only.
Prevent unauthorized access to the Lockbox.	Change the Lockbox password immediately after installation to best protect its contents.
Limit which users have write privileges to the config directory.	Limit access to the `<SYMAPI_HOME>/config` directory to authorized users only. All other users should have limited access (read-only or no access, if possible) to this directory.
Minimize injection attacks and other issues.	Use the `daemon_options secure_directory_path` to specify which output directories daemons may write to.

Table 3 Solutions Enabler security configuration checklist (continued)

Purpose of activity	Task
Securing daemons	
Reduce system exposure by using non-root execution of daemons.	Use the `stordaemon setuser` command to establish a non-root user for daemons, and directory permissions.
Securing SRM operations	
Limit access to SRM functionality.	Limit permission to the SRM daemon. Edit the common daemon authorization file, `daemon_users`.
Limit security exposure by using a database account in SRM with minimal privileges.	Configure a minimally privileged account for SRM database access
Protect directories and files.	Restrict access privileges for directories and files.
Start up and shut down the database server manager instance.	Configure database startup options.

SYMAPI home and bin directory locations

The Solutions Enabler `<SYMAPI_HOME>` and `<SYMCLI_BIN>` directories are found in the following locations by default:

<SYMAPI_HOME>

- `Windows: c:\Program Files\EMC\SYMAPI...`
- `UNIX: /var/symapi/...`
- `z/OS: /var/symapi/...`

Pathnames presented in this document use a UNIX-specific format: forward slashes (/) instead of the backslashes (\) typically used on Windows platforms.

<SYMCLI_BIN>

- `Windows: C:\Program Files\EMC\SYMCLI\bin...`
- `UNIX: /usr/storapi/bin...`

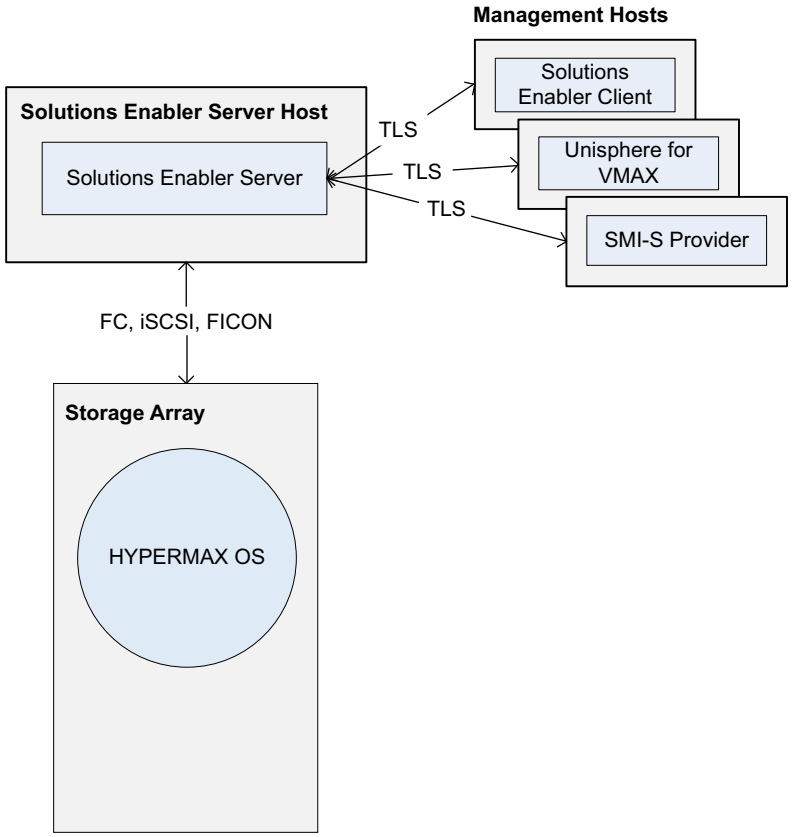
Note

By default, the location of `<SYMAPI_HOME>` is the same for both z/OS and UNIX. The *EMC Solutions Enabler Installation and Configuration Guide* provides more information about:

- Changing the location for `<SYMAPI_HOME>` on z/OS systems during installation.
- Open VMS file locations.

Security controls map

Figure 2 Solutions Enabler components



Access control

Solutions Enabler provides two mechanisms to control access to arrays: host-based access and user-based access.

- The `symacl` command provides host-based access control that can restrict host access to selected sets of devices across multiple arrays. Host-based access control limits the management operations a host can perform and provides highly granular control over management operations. Functionality provided by the `symacl` command is referred to as Symmetrix Access Control.
- The `symauth` command provides user-based authorization that assigns a user or group to a role. Roles limit the management operations users can perform on an array.

Note

When configuring Symmetrix Access Control, it is important to:

- Give access rights only to authorized hosts.
- Assign only the privileges users require to perform their tasks.
- Grant ADMIN rights to a very limited number of users (for example, assign ADMIN rights to only known users and a select administrative group).

The *EMC Solutions Enabler Array Controls and Management for HYPERMAX OS CLI User Guide* provides information on how to set up and perform host-based access control and user-based authorization with the `symacl` and `symauth` commands.

Host access IDs

Symmetrix Access Control identifies individual management hosts using access IDs which are stored in a Lockbox. The Lockbox is associated with a particular host which prevents copying the Lockbox from one host to another. There are two different methods to generate the access IDs:

- Alternate access ID: The host's access ID can be generated at random or from a user-defined passphrase, then stored in a secure location on the local disk. Alternate access IDs are supported for all platforms. See Alternate access IDs on page 28 for more information on alternate access IDs.

  Note

  It is strongly recommended that you use alternate access IDs on platforms where the hardware-based access ID is derived from a network interface MAC address.

- Hardware-based access ID (default): The host's access ID is derived from hardware characteristics of that host:
  - On x86_64 (64-bit Intel/AMD), and IA 64 platforms, a network interface MAC address is used.
  - On other platforms, characteristics of the host, such as a processor identifier, are used.

Note

When MAC addresses generate access IDs, the IDs may be unreliable or ineffective under some circumstances, including clustering environments, virtual environments, or following a hardware change. For added security on x86_64 (64-bit), IA64, and BS2000 hardware platforms, it is strongly recommended that you use alternate access IDs instead of hardware-based access IDs.

Alternate access IDs

Alternate access IDs are available for all platforms. When alternate access IDs are enabled, Solutions Enabler can:

- Randomly generate an access ID.
- Generate an access ID based on a user-chosen passphrase, where the passphrase is either:
  - Entered on the command line in an option.

- Entered in a file, whose name is specified in the command line.

You enable alternate access IDs with the SYMAPI_ALTERNATE_ACCESS_ID option in the *<SYMAPI_HOME>*/config/options file.

Solutions Enabler securely stores the alternate access ID on the local disk in the Lockbox file. The symacl man page provides more information on the symacl -unique command.

Note

Solutions Enabler access control changes must be made from an administrative host with ADMIN rights to the array and rights to make symacl changes.
If you only have one such administrative host, and you change its alternate access ID, once that change is made, the host can no longer make access control changes because the new access ID is not yet in an access group.

It is recommended that you enable a second administrative host prior to attempting to change a host's alternate access ID.

User-based access control

User authorization assigns individual users to roles to limit the management operations that users can perform. User-based controls are less granular than host-based controls.

You can use the symauth command, Symmetrix Management Console (SMC), or Unisphere for VMAX to assign users to roles.

Solutions Enabler does not support an explicit authentication mechanism for users. It uses the credentials that users supply when logging onto the local system, as provided by the operating system. SMC and Unisphere for VMAX pass the user's authenticated identity to Solutions Enabler.

For information on the symauth command, see the *EMC Solutions Enabler Array Controls and Management for HYPERMAX OS CLI User Guide*.

For information on managing Unisphere for VMAX user accounts, see the *EMC Unisphere for VMAX Installation Guide*.

User identification

Internally, Solutions Enabler represents a user identity as a string assembled from the user's name and authentication source. The possible encodings are:

H:HostName \UserName	A user authenticated by the local operating system.
D:DomainName \UserName	A user authenticated by a specific domain on Windows.
L:ServerName \UserName	A user authenticated by an LDAP server. (SMC or Unisphere for VMAX.)
C:HostName \UserName	A user authenticated by the private SMC or Unisphere for VMAX authentication service on some host.
M:Symmetrix ID \UserName	A user authenticated by a management guest host running on the specified Symmetrix array.

Solutions Enabler uses these identities in a number of ways. A username is included in records written to the array's secure audit log. This identifies the user that initiated

the activity being logged. A user identity is the basis for optional user authorization rules that restrict management access to arrays.

Support for all user groups

Solutions Enabler checks all groups a user belongs to. During rights checking, each user group is examined for a role mapping and the “or” of all rights granted to each group.

The `symauth show –username` command displays all groups a user belongs to.

Authorization rules can be configured for an array that map either a user or group name to a management role.

For both user and group authorization, the contained name can be fully qualified (such as `D:Corp\Jones` and `D:Corp\Sales`) or unqualified (such as Jones and Sales).

The rights that are called out for any of these entries matching the user's identity are granted to that user.

Authorization entries with an unqualified group name are only considered if there are no group entries with a fully qualified name matching the user.

The `symauth` man page provides more information on this topic.

Multiple authorization roles

In Solutions Enabler 8.x, you can use the `symauth` command to assign up to four authorization roles. Each role is separated with a '+' character. For example:

```
StorageAdmin+Auditor+Monitor
```

Output of the `symauth list` command displays authorization roles ordered from most powerful to least powerful. For example:

```
StorageAdmin+Auditor+PerfMonitor
```

Backward compatibility

Solutions Enabler versions 7.6 and earlier support only one role per user or group. To make later versions compatabile with versions 7.6 and earlier, you must create at least one authorization rule that corresponds to the version 7.6 roles of Admin or SecurityAdmin. This ensures that older versions of Solutions Enabler can interpret at least one rule.

When a user has multiple roles defined on an array running Solutions Enabler 8.x, older versions of Solutions Enabler display only one (the highest assigned) role for that user.

Considerations when deleting or modifying rules

Users on pre-8.x systems can modify the rules on systems running Solutions Enabler 8.x, but the following cautions apply:

- Users on pre-8.x systems can see only one (the highest) role of a rule on a system running Solutions Enabler 8.x, even if the 8.x rule contains multiple roles.
- If a user on a pre-8.x system deletes a rule on an 8.x system that contains multiple roles, the operation deletes the entire multiple role rule.
- If a user on a pre-8.x system modifies a rule on an 8.x system that contains multiple roles, the modification replaces the multiple roles in the rule with the single role specified by the pre-8.x user.

Example: A rule on a system running Solutions Enabler 8.x contains both StorageAdmin and Monitor roles.

In this case, a user on a pre-8.x system can see only the StorageAdmin role. If the user modifies the rule to Auditor role, both the StorageAdmin and Monitor roles are

removed even though the pre-8.x system sees only the StorageAdmin role in the rule before the modification.

Client/server access IDs

Anyone with access to array management software can execute functions on any of the array's devices. Many applications can issue management commands to any device in a deployment. Such shared systems may be vulnerable to a host accidentally or intentionally tampering with another's devices. To prevent this, you should set up and restrict host access to defined sets of devices across the arrays.

By default, client/server mode operations are executed on the server host using the access ID of the server. Access control checks are performed against the rules established for the server host, regardless of which client host initiated the operations.

You can use the access ID of the client host instead of the server host to perform this check. When this is enabled, access control rules must be established for, and checked against, the client hosts from which the operations are issued.

To use the access ID of the client host, you must make changes in the `<SYMAPI_HOME>/config/options` file on the client and the server host. On the server, the SYMAPI_USE_ACCESS_ID option controls the source of the access ID used for the client/server sessions. On the client, the SYMAPI_ALTERNATE_ACCESS_ID option must be enabled to use alternate access IDs. Use the SYMAPI_CLIENT_SIDE_ACCESS_ID to control whether the client can send its own access ID to the server. By default the SYMAPI_CLIENT_SIDE_ACCESS_ID option is disabled (the client does not send its access ID to the server in client/server mode).

For more information on setting server or client host access ID, see the *EMC Solutions Enabler Array Controls and Management for HYPERMAX OS CLI User Guide*.

Solutions Enabler log files

Solutions Enabler maintains three types of log files:

- Secure audit log – The secure audit log records configuration changes, security alarms, service operations, and security-relevant actions on the array.
- SYMAPI log files – The SYMAPI log file records SYMAPI errors and other significant conditions. One log file is created per day using a date format. A new log file is started everyday on the first write after 12:00 am.
- Daemon log files – The daemon log files record daemon errors and other significant conditions. Each deamon has two log files (.log0 and .log1). Logging alternates between the two files, switching to the other file each time the maximum size specified by the daemon's LOGFILE_SIZE parameter is reached. Each daemon writes to the .log0 file until its size exceeds that specified in the LOGFILE_SIZE option, at which point it switches to the .log1 file. It switches back to .log0 under the same conditions.

For more detail on log files, see the *EMC Solutions Enabler Array Controls and Management for HYPERMAX OS CLI User Guide*.

Port usage

This section describes the ports Solutions Enabler uses to communicate between server and client hosts.

If a firewall or network address translator is present, these ports must be open. Typically, this is a firewall between the Solutions Enabler client and the server hosts.

Server ports
In client/server mode, the Solutions Enabler server (storsrvd daemon) listens by default at TCP/IP port 2707 for client connections.

You can configure a port by adding an entry to *<SYMAPI_HOME>*/config/daemon_options file. If you change the default port at the server, you must modify the *<SYMAPI_HOME>*/config/netcnfg configuration file at client hosts to reflect the use of the non-default port.

To change the server port the server must be down. To use a different port, specify it in the daemon_options file, then restart the storsrvd daemon.

Event daemon ports
When using the asynchronous events in client/server mode, the event daemon at the client host listens at a TCP/IP port for events being forwarded from the event daemon at the server. By default, the client event daemon asks the operating system to pick an unused port for it to use.

You can configure a specific port to use by adding an entry to the *<SYMAPI_HOME>*/config /daemon_options file on the client host. The event daemon uses the following ports by default:

Port	Description
Dynamically assigned 1024 - 65535	In client/server mode, the event daemon (storevntd) on a client host listens on this port for asynchronous events sent to it from a server host. By default, this is picked at random by the client host event daemon.
514	Port the server listens on for events.
162	Port the application listens on for traps.

Client/server security settings

In Solutions Enabler client/server mode, client host operations are automatically forwarded to the storsrvd daemon on a server host for execution.

By default, traffic transmitted between client and server hosts is encrypted using TLS/SSL.

This section describes the mechanisms to operate these connections in a secure manner.

Network encryption

Platforms where Solutions Enabler supports secure sessions default to securing all connections using TLS/SSL.

v8.1 and higher uses OpenSSL with the OpenSSL FIPS Object Module 2.0 (NIST certificate #1747). OpenSSL support is as follows:

- v8.4 - OpenSSL 1.0.2j
- v8.2 - OpenSSL 1.0.1q

- v8.1 - OpenSSL 1.0.1p

FIPS mode is supported on the following platforms:

- Linux x86 platforms
- Windows x86 64 bit platforms

The version of TLS varies depending on the version of Solutions Enabler:

- v8.0.2 server and a client 7.6.2 or later - Client and server use TLS V1.2 with Advanced Encryption Standard (AES) with 128-bit key, Galois Counter Mode (GCM), with Secure Hash Algorithm 1 (SHA-1).
  In v 8.0.2 SSLv2 and SSLv3 are disabled by both the client and server. Sessions are secured using TLS v1.0 or TLS v1.2.
- v8.4 - TLSv1 and TLSv1.1 are disabled by both client and server. Sessions are secured using TLSv1.2 only.
  v8.4 also disables all SHA1 ciphers. Only AES128 GCM with SHA256 ciphers are used.

Note

FIPS 140-2 mode is enabled by default.

Securing remote connections using TLS/SSL

For platforms that support secure SYMAPI client and server communications, the default/initial configuration is to negotiate only SECURE sessions. You can modify the security level at which the client and server are operating.

Before modifying the security level, you should:

- Understand that the security level specifies the capability of the local side and the local side's expectation of the remote side.
- Know whether the host is SSL-capable or SSL-incapable.

The possible security levels are:

- Level 3 (SECURE) — (Default) Indicates that only secure sessions will be negotiated between the client and server. This is the highest level of security, and it should only be used when there is no chance of an SSL-incapable client attempting to connect with the server, or an SSL-capable client connecting to an SSL-incapable server.
- Level 2 (ANY) — Indicates that either secure or non-secure sessions will be negotiated between the client and server on SSL-capable platforms.
- Level 1 (NONSECURE) — Indicates that only non-secure sessions will be negotiated between the client and server. This level is intended as a last resort in situations where SSL cannot be used for some reason or is undesirable. In addition, this level can also be useful in matters of performance and availability.

The default security level is SECURE on platforms that support secure communications and NONSECURE on platforms that do not support secure communications. The following messages may be issued by the server if SSL-related problems occur:

- ANR0141E through ANR0145E
- ANR0147E
- ANR0148E
- ANR0150E through ANR0153E

- ANR0155E

The *EMC Solutions Enabler Installation and Configuration Guide* provides details about SYMAPI server daemon messages.

Session negotiation behavior

The following table details the type of session negotiated if a client and server are at the same or different security levels (implied or configured).

Table 4 Session negotiation behavior

Client security level	Server security level	Negotiated session type
SECURE	SECURE	SECURE
	ANY	SECURE
	NONSECURE	Rejected
NONSECURE	NONSECURE	NONSECURE
	ANY	NONSECURE
	SECURE	Rejected
ANY	ANY	SECURE
	SECURE	SECURE
	NONSECURE	NONSECURE

Server host security

Note

It is strongly recommended to synchronize host times for the server and client hosts before generating and using OpenSSL certificates. Failure to synchronize host times could result in difficulty in establishing secure connections.

You can configure server host security levels in two ways:

- Use the SYMAPI_SECURITY_LEVEL option in the `<SYMAPI_HOME>/config/options` file. This option specifies whether the server accepts only secure sessions from clients.
  The default value for the SYMAPI_SECURITY_LEVEL option is SECURE. The server accepts only secure sessions from clients.
- Use the SECURITY_LEVEL parameter in the `<SYMAPI_HOME>/config/daemon_options` file. The default for the SECURITY_LEVEL parameter is SECURE.

If both the SYMAPI_SECURITY_LEVEL option in the `options` file and SECURITY_LEVEL parameter in the `daemon_options` file are set, and are set to different levels, then the setting on the SYMAPI_SECURITY_LEVEL option in the `options` file overrides the setting on the SECURITY_LEVEL parameter in the `daemon_options` file.

NOTICE

It is strongly recommended that you use secure sessions. Non-secure sessions are not recommended, however, you can allow non-secure sessions from clients by modifying the SYMAPI_SECURITY_LEVEL or SECURITY_LEVEL options.

FIPS 140-2 encryption

To set whether to operate in FIPS 140-2 mode for client/server communication, use the SYMAPI_FIPS option in the *<SYMAPI_HOME>*/config/options file. When the SYMAPI_SECURITY_LEVEL option is set to SECURE, the SYMAPI_FIPS option enables or disables FIPS 140-2 compliant encryption of Solutions Enabler client/server sessions on Linux and Windows platforms. The default value for the SYMAPI_FIPS option is ENABLE.

For a full description of the SYMAPI_SECURITY_LEVEL and SYMAPI_FIPS options, see the *EMC Solutions Enabler CLI Reference Guide*.

Backward compatibility to pre-8.0 configuration files

Solutions Enabler 8.0 provides backward compatibility to 7.5 and earlier versions using the following logic to select the security level:

- Look for SYMAPI_SECURITY_LEVEL in the *<SYMAPI_HOME>*/config/options file.
- If SYMAPI_SECURITY_LEVEL is specified in the *<SYMAPI_HOME>*/config/options file, use it.
- If the SYMAPI_SECURITY_LEVEL security level is not specified in the *<SYMAPI_HOME>*/config/options file, the server looks for storsrvd:security_level in the *<SYMAPI_HOME>*/config/daemon_options file.
  - If the storsrvd:security_level is not specified on the server, look for SYMAPI_SERVER_SECURITY_LEVEL.
    - If the SYMAPI_SERVER_SECURITY_LEVEL is not specified, use the default for the platform: SECURE everywhere except OVMS, BS2000, or IBM i, which use NONSECURE.
    - If the SYMAPI_SERVER_SECURITY_LEVEL is specified, use the specified value and post a message saying it was used instead of the storsrvd:security_level.
  - If the storsrvd:security_level is specified, use it.

Verifying client security certificates

By default, if a client has a subject certificate, a server requires the certificate and verifies it. This behavior is controlled by the SECURITY_CLT_SECURE_LVL parameter in the *<SYMAPI_HOME>*/config/daemon_options file.

The default value for the SECURITY_CLT_SECURE_LVL parameter is VERIFY.

For a full description of the SECURITY_CLT_SECURE_LVL parameter, see the *EMC Solutions Enabler CLI Reference Guide*.

Client host security

By default, a Solutions Enabler client attempts to negotiate a secure session with the server when both the server and client are capable of secure sessions. It is not recommended that you disable secure communications, however, if you need to allow non-secure sessions between a client and server that cannot negotiate a secure

session, you can modify the SYMAPI_SECURITY_LEVEL option in the *<SYMAPI_HOME>*/config/options file to allow non-secure sessions.

netcnfg file

To configure session security for specific server hosts, modify the *<SYMAPI_HOME>*/config/netcnfg file for the server in question. This file maps service names to server hostnames (or IP addresses) and port numbers for Solutions Enabler SYMCLI commands. If you do not specify a security level, SECURE is used for secure-capable platforms, and NONSECURE is used for secure-incapable platforms, depending on the configuration of the server.

If both the SYMAPI_SECURITY_LEVEL option in the options file and the security level in the netcnfg file are set, and are set to different levels, then the security level in the netcnfg file takes precedence over the setting in the options file.

For more information on the security settings in the options and netcnfg files, see the *EMC Solutions Enabler CLI Reference Guide*.

Secure session configuration summary

The following table lists the host operating systems that support SSL.

Table 5 Host operating systems that support SSL

Operating systems that support SSL
AIX (64-bit)
HP-UX (64-bit) HP-UX Itanium (64-bit)
Linux Itanium (64-bit) Linux AMD (64-bit)
Solaris (64-bit)
Windows AMD (64-bit)
z/OS

Note

Solutions Enabler does not support SSL on iSeries, BS2000, or OpenVMS.

The following table provides a summary of the secure session settings. See the *EMC Solutions Enabler CLI Reference Guide* for more information.

Table 6 Secure sessions summary

Option name, possible values, and location	Description
storsrvd:security_clt_secure_lvl =MUSTVERIFY |VERIFY |NOVERIFY *<SYMAPI_HOME>*/config/daemon_options	On server hosts, controls how the server validates client certificates.

Table 6 Secure sessions summary (continued)

Option name, possible values, and location	Description
	Note This option is not supported on z/OS hosts, where it defaults to NOVERIFY. MUSTVERIFY: The server requires clients to send a valid certificate. VERIFY (default): The server verifies a client's certificate, if one is sent. NOVERIFY: The server does not verify client certificates.
storsrvd:security_level =SECURE | NONSECURE |ANY *<SYMAPI_HOME>*/config/daemon_options	On server hosts, controls whether servers establish a secure session. SECURE (default): Secure sessions are always used. All other connection types are refused. NONSECURE: Non-secure sessions are used; secure sessions are not used. ANY: A secure session is established when supported by the client; otherwise a non-secure session is used.
SYMAPI_SECURITY_LEVEL = SECURE | ANY | NONSECURE *<SYMAPI_HOME>*/config/options	Specifies whether the Solutions Enabler server accepts only secure sessions from clients. Applies to both server and client. SECURE (default): Secure sessions are always used. All other connection types are refused. NONSECURE: Non-secure sessions are used; secure sessions are not used. ANY: A secure session is established when supported by the client; otherwise a non-secure session is used.

Certificate files

Solutions Enabler uses OpenSSL to generate certificates for secure client-server communication. The client and server verify each other's identity based on the information contained in the certificates.

During installation, you have the option to install the certificate component. If you choose to install the certificate component, a default set of certificates is generated. These certificates are signed by a self-signed root certificate.

Solutions Enabler uses a root certificate and key to generate subject certificates that identify client and server hosts. The root certificate is installed on the host. The

installation process automatically generates a subject certificate for the host on which the install is executed.

The generated certificates can be replaced with certificates that you generate or that are issued to you by a commercial certification authority.

Subject certificates are generated for both client and server hosts. The subject certificates represent the identity of the host without respect to whether the host acts as a client or a server. A single set of certificates can be used in both the client and server.

The client and server can be configured separately to use other sets of certificates. By default, both the client and the server validate the certificate of the peer during secure session negotiation. The client always validates the server's certificate; you cannot disable this validation when a secure session is negotiated.

The `cert` directory is located at:

- Windows: *<SYMAPI_HOME>*`\config\cert`
- UNIX and z/OS: *<SYMAPI_HOME>*`/config/cert`

Note

By default, the location of cert directory is the same for z/OS as UNIX. The location for z/OS systems can be changed during installation.

The following certificate files enable a client to verify a server's identity and a server to verify a client's identity:

- `symapisrv_cert_v8.*.pem` is the default version 8.* subject certificate file where 8.* is the Solutions Enabler version. It is created specifically for its particular host during installation. It is signed by the EMC Enterprise Storage Automation root certificate symapisrv_trust_vn.n.pem. This file must be in the `cert` directory on the SYMAPI client and server for client/server security to work.
- `symapisrv_trust_v8.*.pem` is the EMC Enterprise Storage Automation Root certificate, where 8.* is the Solutions Enabler version. This file must be in the cert directory on every client and server.
- `symapisrv_key_v8.*.pem` is the key file associated with the subject certificate, where 8.* is the Solutions Enabler version. It is created specifically for its particular host during installation. It is generated during the certificate creation process. This file must be in the cert directory on the SYMAPI client and server for client/server security to work.

Solutions Enabler v8.0.x-8.3.x support backward compatibility with pre-v8.0. For backward compatibility with pre-v8.0 versions the following certificate files are also created in the cert directory:

- `symapisrv_cert.pem` is the pre-V8.x subject certificate file. It is created specifically for its particular host during installation. It is signed by the EMC SPEA pre-V8.x Root certificate. This file must be in the cert directory on the SYMAPI client and server for pre-V8.x client/server security to work.
- `symapisrv_trust.pem` is the EMC SPEA pre-V8.x Root certificate used to sign the SYMAPI certificate file. This file must be in the cert directory on every client and server for pre-V8.x client/server security to work.
- `symapisrv_key.pem` is the pre-V8.x key file associated with the subject certificate. It is created specifically for its particular host during installation. It is generated during the certificate creation process. This file must be in the cert directory on the SYMAPI client and server for pre-V8.x client/server security to work.

Note

Solutions Enabler v8.4 and higher does not support certificates generated prior to Solutions Enabler v8.0.

Managing backward compatibility of certificates

Note

This section applies to Solutions Enabler v8.0.x-8.3.x. Solutions Enabler v8.4 and higher does not support certificates generated prior to Solutions Enabler v8.0.

Solutions Enabler 8.x is backward compatible with certificates generated by earlier versions, back to 7.4. For example:

- A Solutions Enabler 8.x server can verify a certificate generated by an older version.
- A Solutions Enabler 7.6 client can verify a server certificate generated with `-san` and `-mode V76` options.
- An older client (Solutions Enabler 7.5 or earlier), can verify a certificate generated by a Solutions Enabler 8.x server if the certificate's CN contains either:
  - A Fully Qualified Domain Name (FQDN) - if the server host name can be resolved to a FQDN
  - An IP address corresponding to the server - if the server host name cannot be resolved to a FQDN

  In cluster configurations, if the Solutions Enabler 8.x server's certificate does not contain wildcards in the CN, the Solutions Enabler 7.5 client will not verify the server if the server fails over and presents a different host ID than that present in the CN.

  If a Solutions Enabler 8.x server is running in a clustered environment, Solutions Enabler 7.5 and older clients must have certificates for each host node of the server cluster.

⚠ CAUTION

When generating certificates on Solutions Enabler 8.x servers, be careful not to add non-DNS host names in the CN if Solutions Enabler 7.5 and older clients will connect to the server.

Server security considerations

Starting up the server

The `storsrvd` daemon does not run by default. You must explicitly start it before it can accept connections from remote clients. You can configure the daemon to start automatically whenever a server host starts.

The *EMC Solutions Enabler Installation and Configuration Guide* provides detailed instructions on starting the Solutions Enabler server.

Restricting access to the server

The `<SYMAPI_HOME>/config/nethost` file on a server host restricts the hosts and users from which the `storsrvd` daemon accepts connections. If the `nethost` file is not present, connections are accepted from all client hosts.

Note

The server considers the contents of the `nethost` file before deciding whether it will negotiate a SYMAPI session with the client. If the client host and user are not defined in the `nethost` file, a session will not be negotiated, regardless of the security level.

The EMC Solutions Enabler Installation and Configuration Guide describes the `nethost` file.

Restricting server functionality

You can use settings in the *<SYMAPI_HOME>*`/config/options` file on a server host to restrict the functionality that the `storsrvd` daemon is allowed to perform on behalf of remote client hosts. Check to make sure all references to the `options` file have a path name of `<SYMAPI_HOME>/config/options`. You can edit the functionality options in the `options` file while the server is running. The running server uses the new settings for all future sessions.

Since the settings are not specified in the *<SYMAPI_HOME>*`/daemon_options` file, they cannot be changed using the `stordaemon setvar` command.

The following table lists the options in the `options` file that restrict `storsrvd` daemon functionality:

Table 7 Options that restrict storsrvd functionality

Option name (in <SYMAPI_HOME>/config/options)	Description
SYMAPI_ACC_ADMIN_VIA_SERVER	Enable/disable Symmetrix Access Control changes. Default is ENABLE.
SYMAPI_ACC_DISPLAY_VIA_SERVER	Enable/disable Symmetrix Access Control information displays. Default is ENABLE.[a]
SYMAPI_ALLOW_SCRIPTS_VIA_SERVER	Enable/disable TimeFinder® pre-action and post-action scripts. Default is DISABLE.
SYMAPI_CTRL_VIA_SERVER	Enable/disable array control operations in general. Default is DISABLE.[a]

a. When set to DISABLE, this class of functionality is not available through the server.

Specifying nodes and addresses

A server can accept connections from IPv4 or IPv6 clients. The exact syntax is important If you specify the network address instead of the node name in the `nethost` file. If you incorrectly specify an address, connections from some clients may be denied.

It is recommended to specify the node name (or the FQDN) since proper DNS configuration usually ensures that the name of the client host is consistent, regardless of the network address.

If you must specify the address, keep these factors in mind:

- The rules for specifying an IPv4 address are simple: Specify the complete address in its dotted-decimal form, without leading zeros in each octet. For example:

```
172.23.191.20      user1
10.243.142.82      user1
```

- If you want to specify an IPv6 address, follow these shorthand rules (part of the IPv6 standard):
  - Leading zeros in each quartet can be omitted.
  - Contiguous sets of zeros can be replaced by two adjacent colons, but only once in an address. If there are multiple non-adjacent sets of contiguous sets of zeros, only one set of double colons can be used. The other set of zeros must be specified. For example:

    ```
    3FFE:80C0:22C:18:250:88FF:FEAD:F92F
    ```

    If you are uncertain about the address syntax, ask your network administrator to determine the exact syntax. For most UNIX and Linux hosts, the `ifconfig -a` command can be used to display the IPv6 address of a machine. In a Microsoft Windows environment, use the `ipconfig /all` command to display the IPv6 address.
- If you have IPv4 client hosts that connect to IPv6-capable servers on AIX or Linux, the client network address appears as IPv4-mapped addresses. The server host file validation logic takes this into account and treats IPv4-mapped addresses as though they are native IPv4 addresses. You can specify the regular IPv4 address as described in the first point above.
- You may have to experiment to find the right address.

Concurrent connections

The maximum number of concurrent connections from client hosts is controlled by the `storsrvd:max_sessions` parameter in the *<SYMAPI_HOME>*`/config/daemon_options` file. When a new session arrives that exceeds the threshold, it is refused.

The default and maximum value is 100.

Concurrent sessions may be limited based on the source hostname or username of the client:

- Limiting by source host is based on the IP address of the host where the client session originates. User name is not considered when counting concurrent connections from hosts.
- Limiting by source user is based on the user identity format. Only two types of user identity formats are counted:
  - The H: format identifies that the client user has been authenticated by the local operating system. This format is used when the client comes from any UNIX or Linux type of host, or from a Windows host where the user has logged into the local system (not a Windows domain). In the host authentication case, the user is considered the same only when logging in from the same host with the same user name.
  - The D: format is used when the client user has logged into a Windows domain. In this case, a user can log into the same domain from different host computers. Such a user identity is considered the same, without respect to the source host that initiates the session.

Two configuration statements for `storsrvd` control session refusal from specific sources:

- `storsrvd:max_sessions_per_host=value` – This option specifies the maximum number of concurrent sessions from any specific host. If a new session from the source host exceeds the threshold for that host, the session is refused.
- `storsrvd:max_sessions_per_user=value` – This option specifies the maximum number of concurrent sessions from any specific user. If a new session from the same user exceeds the threshold for that user, the session is refused.

Table 8 on page 42 lists the storsrvd session control options and values.

Note

These options and values are only used by the `storsrvd` daemon and apply to SYMAPI remote sessions. There is no impact on the use of the `stordaemon` control CLI or any other Solutions Enabler daemon.

Best practices for setting the `storsrvd` session control options:

- Set `max_sessions_per_host` and `max_sessions_per_user` to a value less than `max_sessions`. Specifically:
  - Set `max_sessions` to the highest number of concurrent sessions you will tolerate without respect to the source host or user of the session.
  - Set `max_sessions_per_host` and `max_sessions_per_user` to lower values, reflecting the maximum number of concurrent sessions from specific sources you will tolerate.
- Both `max_sessions_per_host` and `max_sessions_per_user` can be used concurrently to count sessions.
- It is possible to set either `max_sessions_per_host` and `max_sessions_per_user` to 0, but doing so refuses all new connections. It is recommended that if you want to refuse all sessions temporarily, set `max_sessions` to 0. To resume accepting new sessions, change `max_sessions` to a non-zero value.

Table 8 storsrvd daemon session control options and values

Option name	Values	Default	Notes
max_sessions	0 – All new sessions are refused. 1 – 100 – Maximum (host and user) sessions allowed.	100	Default of 100 is compatible with previous releases.
max_sessions_per_host	0 – All new sessions are refused. 1 – 100 – Maximum number of sessions allowed from a specific host. NOLIMIT -Disables counting of sessions from a specific host.	NOLIMIT	NOLIMIT value provides backward compatibility. NOLIMIT is case-insensitive: NOLIMIT = nolimit

Table 8 storsrvd daemon session control options and values (continued)

Option name	Values	Default	Notes
max_sessions_per_user	0 – All new sessions are refused. 1 – 100 – Maximum number of sessions allowed from a specific user. NOLIMIT – Disables counting of sessions from a specific user.	NOLIMIT	

Control operations for IBM z/OS

By default, a Solutions Enabler server running on any z/OS host allows configuration changes when requested by a remote client. The *EMC Solutions Enabler Installation and Configuration Guide* provides additional information.

NOTICE

If control operations are left enabled by default, remote Open Systems users (client/server mode) can make changes to the array configuration on your mainframe system.

File backup

Solutions Enabler maintains important configuration data in a number of files. It is important that you back up and protect these files at all times. If lost, functionality that depends on the data in these files may be impacted.

Back up the following directories and their contents to preserve the Solutions Enabler configuration on a host:

- `<SYMAPI_HOME>/config`
- `<SYMAPI_HOME>/db`
- `<SYMAPI_HOME>/gns`

If you want to retain the logs for audit purposes, include the *<SYMAPI_HOME>*`/log` directory in your backups.

Other directories under *<SYMAPI_HOME>* contain less critical data that is recreated by Solutions Enabler as needed.

The following table lists specific files you should regularly back up.

File location	Description
<SYMAPI_HOME>`/config/emcpwddb.dat`	This file stores connectivity information (including user names and passwords) used to interact with CLARiiON storage arrays and VMware/Hyper-V Virtual Infrastructure Services.

File location	Description
	It is managed using the `symcfg authorization` SYMCLI command. The file is encrypted to protect its contents and prevent tampering.
SYMAPI_HOME>/db/symapi_db.bin	The Solutions Enabler database file contains array topology information; arrays, devices, directors, and other information.
<SYMAPI_HOME>/config/lockboxp2	This file contains sensitive configuration information. The file is encrypted to protect its contents to prevent tampering.
<SYMAPI_HOME>/gns/storgnsd.db	The Solutions Enabler groups database file contains information about CG's, DG's and their contents.

File protection

Solutions Enabler stores its configuration files in the following directory:

<SYMAPI_HOME>`/config`

Protect the files in the `config` directory by making sure only authorized administrators have write access. All other users should have no access or read-only access.

Non-privileged user command use

Following an initial installation of Solutions Enabler, most SYMCLI commands can only be run as a root user on UNIX systems and by an administrator on Windows systems. To allow other users to execute these commands (for example, `symcfg discover`), you must grant them write access to the following directories and their contents:

`<SYMAPI_HOME>/config`

`<SYMAPI_HOME>/db`

In addition, non-root users on UNIX and non-administrators on Windows must be authorized (using the `stordaemon` command) to manage daemons, and to use daemons in the process of running SYMCLI commands. To authorize these users, add an entry for a specific user in the file *<SYMAPI_HOME>*`/config/daemon_users`. For example:

```
# Allow user 'jones' to make use of the storapid daemon:
jones    storapid
# A '*' character at the end of a name can be used
# as a simple wildcard. The following allows user 'jones'
# to make use of any of the Solutions Enabler daemons:
jones    stor*
```

Lockbox

Solutions Enabler uses a Lockbox to store and protect sensitive information. The Lockbox is associated with a particular host. This association prevents the Lockbox from being copied to a second host and used to obtain access.

The Lockbox is created at installation. During installation, the installer is prompted to provide a password for the Lockbox. If no password is provided at installation, a default password: *nodename*@SELockbox1 is generated and stored in the Lockbox along with Stable System values (SSVs, a fingerprint that uniquely identifies the host system). The host_name is the same value as returned by the hostname command.

Stable System Values (SSVs)

Stable System values (SSVs) validate access to the Lockbox. When data is written to or retrieved from the Lockbox, the SSVs in the Lockbox are compared against the SSVs generated from the host. If the SSVs match, the operation is permitted. If the SSVs do not match, the operation fails.

When Solutions Enabler is upgraded, product information in the existing Lockbox is automatically copied into the Lockbox when the Lockbox is first accessed.

When any of the following occur, the host fingerprint may no longer match, and the SSVs inside of the Lockbox must be reset:

- The host is upgraded (either hardware or software)
- The Lockbox file is moved to another host
- User clones a virtual machine

NOTICE

To improve security, change the Lockbox password after resetting the SSVs.

Lockbox passwords

If you create the Lockbox using the default password during installation, change the password immediately after installation to best protect the contents in the Lockbox.

For maximum security, select a password that is hard to guess. It is very important to remember the password.

⚠WARNING

Loss of this password can lead to situations where the data stored in the Lockbox is unrecoverable.

Passwords must meet the following requirements:

- 8 - 256 characters in length
- Include at least one numeric character
- Include at least one uppercase and one lowercase character
- Include at least one of the following non-alphanumeric characters: ! @ # % & Lockbox passwords may include any character that can be typed in from US standard keyboard.
- The new password must not be the same as the previous password.

Default Lockbox password

When you install Solutions Enabler, you are asked whether you want to use the default password for the Lockbox. If you choose to use the default, the installation process establishes the default Lockbox password in the following format:

nodename@SELockbox1

where: *nodename* is the hostname of the computer on which you are installing.

Operating systems have different methods of determining the node name:

- Unix: The installation program uses the hostname command to determine the node name. Normally, the node name is set in the `/etc/hosts` file.
- Windows: The value of the COMPUTERNAME system environment variable, converted to lower case.
- z/OS: The gethostname() function is used to get the node name of the machine.

If the value of *nodename* is stored in upper case letters, it is converted to lower case for the default password.

NOTICE

It is strongly recommended that you change the default password. If you allow the installation program to use the default password, note it for future use. You will need the password if you need to reset the Lockbox Stable System values or generate certificates for client/server operations.

Password and SSV management

SSVs are platform-dependent. Changes to hardware or software on a host may require you to reset the SSVs stored in the Lockbox.

Lockbox administrative interactions include:

- Changing the password used to protect the Lockbox.
- Resetting the saved SSVs in the Lockbox after attributes on the host change, making the Lockbox inaccessible to user-initiated SYMAPI and SYMCLI calls.

Note

You must restart all Solutions Enabler daemons after changing or resetting the Lockbox password.

Two `symcfg` commands allow administrative interactions with the Lockbox:

```
symcfg -lockbox [-password <Password>]
   reset -ssv
   setpw [-new_password <NewPassword>]
```

Note

Both commands require the existing password.

Daemon security settings

Solutions Enabler uses a number of helper daemon processes:

- storapid
- storevntd
- storgnsd
- storrdfd
- storsrmd
- storsrvd
- storstpd

- storwatchd

Daemon identity on UNIX

On UNIX, daemons run as a root user by default.

Some daemons can be configured to run as an identity other than a root user. The daemons that may run as a non-root user are:

- storevntd
- storgnsd
- storrdfd
- storsrvd
- storstpd
- storwatchd (Unix only)

Note

The storapid (base) daemon must run as root.

You can configure daemon user identiy at the following times:

- During installation, in either the interactive or silent install process. Refer to the *EMC Solutions Enabler Installation and Configuration Guide* for how to choose non-root daemon execution during installation.
- Post-installation using the `stordaemon` command. For information on which daemons are affected by this option, refer to the stordaemon man page.

If you are running daemons as a non-root user:

- When configured to run as a non-root user, all daemons must run as the same user.
- `stordaemon setuser` sets the UNIX setuid bit on the daemon executables to the named user.
- `stordaemon setuser` alters permission s of directories and files under `/var/symapi` such that the named user can create and delete, read, write the files it needs during normal operation.

To configure all daemons to run under the bin user account:

```
stordaemon setuser all -user bin
```

Authorized users are allowed to control daemons using the stordaemon command line utility. For example, to start the SRM daemon:

```
stordaemon start storsrmd
```

Non-root and non-administrative users must be defined in the `daemon_users` file to obtain authorization for using daemons and other daemon services.

For additional information, refer to:

- The stordaemon man page.
- *<SYMAPI_HOME>*`/config/README.daemon_users` file installed with Solutions Enabler.

Secure host directories

The Solutions Enabler daemons can run with root privileges for UNIX systems and system account file privileges for Windows systems.

These privileges are typically greater than the privileges granted to users making use of the daemon processes. This can present security vulnerabilities in situations where a user through a CLI or some other application provides a pathname on which a daemon can operate, such as a backup file to be written to or read from.

To prevent these security vulnerabilities for the `storsrvd` daemon running as a root user, you can specify a list of secure directories in which the `storsrvd` daemon can read, write, and execute files. Existing mechanisms protect the Solutions Enabler database and log file locations. Specify a list of secure directories for the `storsrvd` daemon to protect other operations, such as backups and restores.

Note

When daemons are running as non-root user, the `secure_directory_path` option is ignored. In this case, the privileges of the non-root user are used when attempting to write output files in specific directories.

Secure directory path

Review the following before specifying a `secure_directory_path` for the `storsrvd` daemon running as a root user:

- The supplied pathname directories must exist when the daemon is started or the `daemon_options` file is reloaded.
  Nonexistent paths are ignored.

  All subdirectories below the specified directories are also treated as being secure.
- A total of 32 secure directory locations can be maintained.
- Once the `storsrvd` daemon has read the `security_directory_path` statement, directories specified cannot be removed without changing the value in the `daemon_options` file and restarting the daemon.
- New directories can be added while the `storsrvd` daemon is running by editing the `daemon_options` file and reloading it using the following command:
  `stordaemon action storsrvd –cmd reload`
- If the `secure_directory_path` option is not present, no security checks are performed.
- The `secure_directory_path` option does not apply to the following path names:
  - Path names provided in the `options` or `daemon_options` files.
    These files are assumed to be protected by an administrator.

    An exception is the path named in the `storstpd:dmn_root_location` option:

    If `storstpd` is running as root, and was started by a non-root user using the `stordaemon` command, `storstpd` validates that the path in the `dmn_root_location` option is also specified in the `secure_directory_path` option.
  - Path names accessed (read or written) by the SYMCLI itself.

In client/server mode, these occur under the identity of the user and are subject to standard access control checks against the user identity.

- Pathnames accessed by an API on the client host in client/server mode because these occur under the identity of the user and are not a security risk.

Windows platforms

On Windows platforms, the secure directory path is a list of directories separated by a semicolon (;). Use the backward slash (\) when specifying each directory name.

To apply the `secure_directory_path` to the `storsrvd` daemon:

```
storsrvd:secure_directory_path = c:\Temp\dir1;c:\Users\SE
```

UNIX platforms

On UNIX platforms, the secure directory path is a list of directories separated by a semicolon (;) or a colon (:). Use the forward slash (/) when specifying each directory name.

To apply the `secure_directory_path` to the `storsrvd` daemon:

```
storsrvd:secure_directory_path = /tmp/dir1;/opt/dir2;/users/se
```

Listing secure directories

To display a list of secure directories in effect for the `storsrvd` daemon:

```
stordaemon getvar storsrvd -name secure_directory_path
```

Daemon connection authorization

By default, daemons only accept connection requests from users running with root or administrator privileges.

For non-root users to use this feature, create a `<SYMAPI_HOME>/config/daemon_users` file (initially installed as `README.daemon_users`) with a list of allowed usernames.

Privileged users are automatically authorized, and do not need to be added to the file. Solutions Enabler daemons make connections between one another. Daemon-to-daemon connections are automatically authenticated and authorized.

For more information on authorizing daemon connections, see the *EMC Solutions Enabler Installation and Configuration Guide*.

SRM daemon connections

Access to SRM functionality is controlled by limiting permission to the SRM daemon. This access is controlled using the common daemon authorization file, *<SYMAPI_HOME>*`/config/daemon_users`.

Note

You should protect this file so that only privileged administrators can modify it.

Users meeting any of the following criteria are permitted to control and use the SRM daemon:

- Authorized users: UNIX users with root access, and Windows users that are a members of the Administrators group
- Users listed in the `daemon_users` file located on each host from which they require access

For any directories and files being accessed for SRM control and mapping operations, operating-system-level permission is required.

For more information on defining SRM operations available to users and setting operating system level permissions, see the *EMC Solutions Enabler SRM CLI User Guide*.

CHAPTER 4

Mainframe Enablers

This chapter contains the following topics:

Overview of Mainframe Enablers

Mainframe Enablers is the umbrella term for the suite of products installed in a z/OS environment to provide control and management of the storage array functions directly on z/OS.

Mainframe Enablers provides a subset of the functionality provided by Solutions Enabler. Existing devices can be managed, but (for example) device creation and mapping are out of scope for Mainframe Enablers.

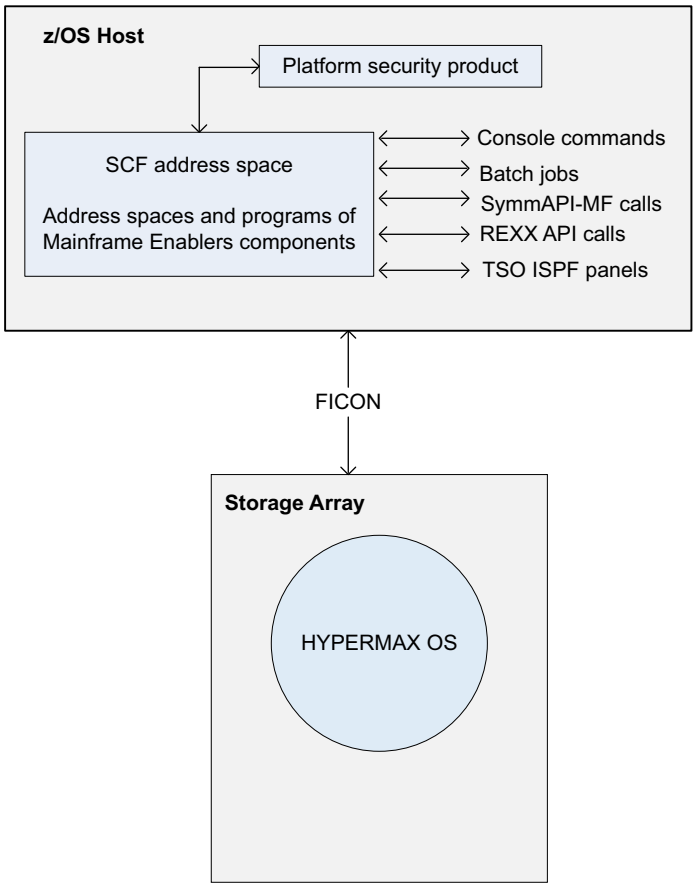
Mainframe Enabler software commands can be executed via:

- Console commands
- Batch job
- Symmetrix API for z/OS (SymmAPI-MF)
- REXX API
- TSO ISPF panels

Symmetrix Control Facility (SCF) is a component of Mainframe Enablers that provides baseline functionality and is a prerequisite for any software control on z/OS. SCF includes SymmAPI-MF for use by EMC and ISV provided products.

Mainframe Enablers 8.0 or greater is required to manage arrays running HYPERMAX OS.

Security controls map



EMCSAFI security interface

Mainframe Enablers use the EMCSAFI security interface to request authorization when a command is executed or a function called. EMCSAFI interface uses RACF 1.9 or higher, or an equivalent SAF-compliant security product. The EMCSAFI interface is enabled by default.

For a full description of EMCSAFI security controls, refer to the EMC Mainframe Enablers Installation and Customization Guide.

Security-related configuration options

Consider the following security-related configuration options:

- SCF initialization file
  The SCF (Symmetrix Control Facility) initialization file can control the storage arrays and devices under SCF management. Refer to the EMC Mainframe Enablers ResourcePak Base for z/OS Product Guide for details.
- z/OS SYMAPI server control restrictions

The RIMLIB member #12CNTRL can limit the functionality provided to SYMAPI clients. Similar to access controls, features can be enabled or disabled to control the services provided by the z/OS SYMAPI server.

CHAPTER 5

Unisphere for VMAX

This chapter contains the following topics:

Unisphere for VMAX checklist

The following checklist summarizes the security-related tasks you should perform to improve the security of your deployment.

Table 9 Unisphere for VMAX security configuration checklist

Purpose of activity	Task
Access control	
Authenticate users with a user account stored on a LDAP-SSL (LDAPS) server.	Set up LDAP-SSL authentication.
User-based access control	
Restrict the management operations users can perform.	Assign users the minimum access they require.
Protect sensitive information	
Update the platform credentials after an upgrade.	Reset the hosts system Stable System Values.
Certificate files	
Replace generated certificates with customer-supplied (trusted) certificates for secure communications.	Replace pre-generated SSL certificates.

SYMAPI home and bin directory locations

The Solutions Enabler `<SYMAPI_HOME>` and `<SYMCLI_BIN>` directories are found in the following locations by default:

<SYMAPI_HOME>

- `Windows: c:\Program Files\EMC\SYMAPI...`
- `UNIX: /var/symapi/...`
- `z/OS: /var/symapi/...`

Pathnames presented in this document use a UNIX-specific format: forward slashes (/) instead of the backslashes (\) typically used on Windows platforms.

<SYMCLI_BIN>

- `Windows: C:\Program Files\EMC\SYMCLI\bin...`
- `UNIX: /usr/storapi/bin...`

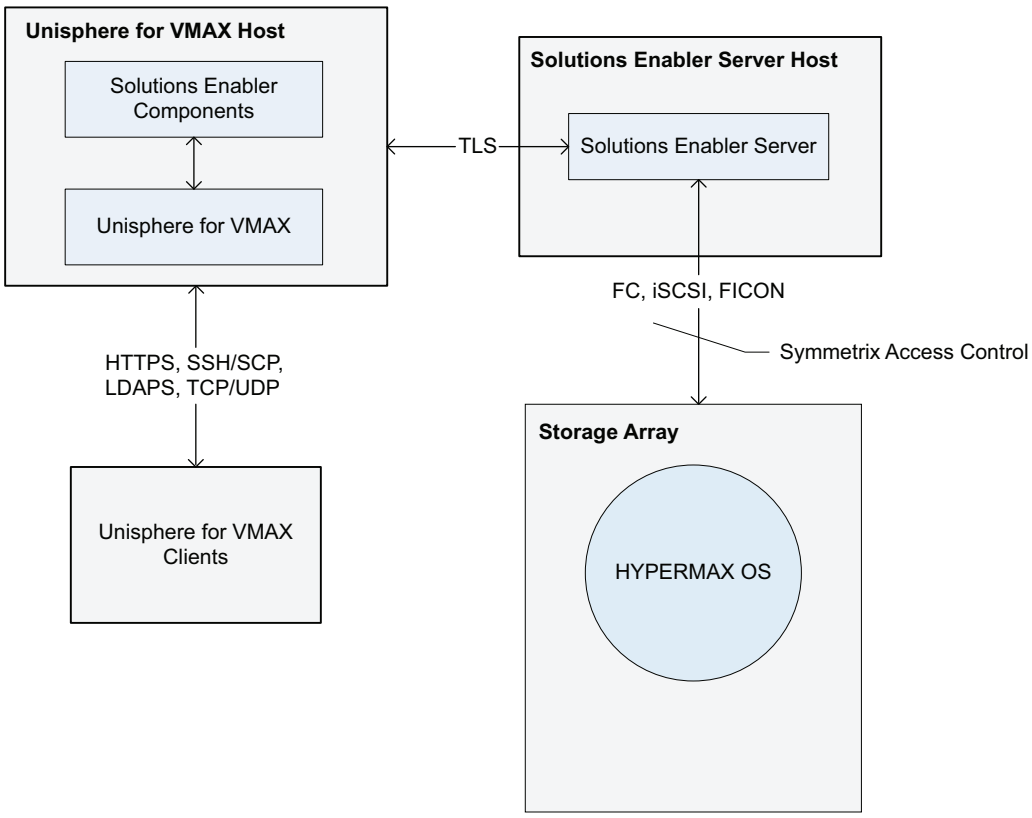
Note

By default, the location of <SYMAPI_HOME> is the same for both z/OS and UNIX. The *EMC Solutions Enabler Installation and Configuration Guide* provides more information about:

- Changing the location for <SYMAPI_HOME> on z/OS systems during installation.
- Open VMS file locations.

Security controls map

Figure 3 Unisphere for VMAX components



Unisphere for VMAX access control

Unisphere for VMAX supports the following types of user authentication:

- Windows (local and domain-based): Users have a Windows account on the Symmetrix Management Application Server (SMAS) server. Users log in with a Windows domain username and password.
- LDAP: User accounts are stored on an LDAP server, which may be accessible over LDAPS (LDAP with TLS1.0, TLS 1.1 or TLS1.2 support). To use this method, a user with Administrator or SecurityAdmin privileges must set up LDAP-SSL authentication in Unisphere for VMAX.

NOTICE

EMC strongly recommends using VPN solutions if the customer's LDAP servers are outside the DMZ, and in cases where the security of the network on which Unisphere for VMAX is operating cannot be guaranteed.

- Local users: Users can have local Unisphere for VMAX accounts. Users log in with their Unisphere for VMAX username and password. Local user accounts are stored locally on the SMAS server host and work in much the same way as the other methods to validate user credentials. To use this method, a Unisphere for VMAX Initial Setup User, Administrator, or SecurityAdmin user must create a local Unisphere for VMAX user account.

The *EMC Unisphere for VMAX Installation Guide* and Unisphere for VMAX online help include instructions on how to create users and configure LDAP authentication.

External EMC applications establish trust in Unisphere for VMAX using the sequence described in Link-and-launch security on page 64.

User-based access control

Unisphere for VMAX uses roles and groups to restrict which management operations a user can perform on an array.

The steps to create and manage user accounts, including user authorization, are described in the *EMC Unisphere for VMAX Installation Guide* and online help.

Default user account

The Initial Setup User is created during installation.

The Unisphere for VMAX installer software creates the Initial Setup User as a temporary local user. The Initial Setup User has an Administrator role, and is used to install and set up Unisphere for VMAX. Once a user with Administrator or SecurityAdmin privileges is assigned to an array, the Initial Setup User can no longer access or view the array from the Unisphere for VMAX console.

NOTICE

EMC recommends that you delete the Initial Setup User after configuring the array.

Instructions for creating the Initial Setup User are described in the *EMC Unisphere for VMAX Installation Guide* and online help.

User roles

Unisphere for VMAX includes the following user roles:

- None - Provides no permissions.
- Monitor - Performs read-only (passive) operations on an array excluding the ability to read the audit log or access control definitions.
- StorageAdmin - Performs all management (active or control) operations on an array in addition to all Monitor operations. This role does not allow users to perform security operations.
- Administrator - Performs all operations on an array, including security operations in addition to all StorageAdmin and Monitor operations.
- SecurityAdmin - Performs security operations on an array in addition to all Monitor operations.

- Auditor - Grants the ability to view, but not modify, security settings for an array (including reading the audit log, symacl list, and symauth) in addition to all Monitor operations. This is the minimum role required to view the audit log.
- Perf Monitor - Performs the same operations as a monitor, with the addition of being able to set performance alerts and thresholds.
- Initial Setup User - Defined during installation, this temporary role provides administrator-like permissions for the purpose of adding local users and roles to Unisphere.

For additional information on user roles and permissions and the Initial Setup User, see the Unisphere for VMAX online help.

symauth rules

You can use the symauth command, Symmetrix Management Console, or Unisphere for VMAX to create the symauth rules. The requirements vary depending on which method you use to create the symauth rule:

- If you use only Unisphere for VMAX to create the symauth rule:
  - After installation use Unisphere for VMAX to create at least one Administrator user.
  - You can use any username/password-credentialed authority to create the Administrator user.
  - This Administrator user ensures that you can use Unisphere for VMAX to create the symauth rules when arrays are added or removed.
- If you use the temporary Initial Setup User to create a symauth rule:
  - After installation create at least one Administrator user on each array.
  - When an array is added, use the Solutions Enabler CLI to create authorization rules for at least one Administrator user on the new array.

Special characters in x.509 client certificates

Solutions Enabler does not support the following characters in the CommonName/ userPrincipalName extracted from a client's X.509 certificate:

@ : ? ; | < > [ ] + = , * / \

These characters are stripped from the client's X.509 certificate. For example:

The userPrincipalName:

John.q.public@anysite.com

Is changed to Unisphere for VMAX username:

John.q.publicanysite.com

The symauth rule must use the stripped username.

Individual and group roles

Users access an array or component directly through a role assignment or indirectly through membership in a user group that has a role assignment.

User groups enable administrators to assign roles to multiple users simultaneously. User groups are created on the SMAS server according to its operating system and assigned roles with Unisphere for VMAX.

If a user has two different role assignments (one as an individual and one as a member of a group), the permissions assigned to the user will be combined.

For example, if a user is assigned a Monitor role and a StorageAdmin role through a group, the user will be granted Monitor and StorageAdmin rights.

User IDs

The following section describes the SYMAPI format to create users and roles.

Note

This format displays in the footer bar of the Unisphere for VMAX GUI, but not in the User/Role list view or creation wizard.

Users and user groups are mapped to their respective roles by IDs. These IDs consist of a three-part string in the form:

`Type:Domain\Name`

In the event that a user is matched by more than one mapping, the user authorization mechanism uses the more specific mapping:

- If an exact match (e.g., `D:sales\putman`) is found, that is used.
- If a partial match (e.g., `D:*\putman`) is found, that is used.
- If an unqualified match (e.g., putman) is found, that is used.
- Otherwise, the user is assigned a role of None.

Valid values for `Type`, `Domain`, and `Name` are as follows:

Type

Type of security authority used to authenticate the user or group. Possible types are:

L

A user or group authenticated by LDAP. In this case, `Domain` specifies the fully qualified name of the domain controller on the LDAP server.

For example: `L:danube.com\FinanceL:danube.com\Finance` indicates that user group `Finance` will log in through domain controller `danube.com`.

Once configured, individual LDAP users and groups can log in to Unisphere for VMAX using a simple username, or simple group name, respectively. For example, `Finance`.

C

A user or group authenticated by the SMAS server.

For example: `C:Boston\Legal` indicates that user group `Legal` will log in through Unisphere sever `Boston`.

H

A user or group authenticated by logging into a local account on a Windows host. In this case, `Domain` specifies the hostname.

For example: `H:jupiter\mason` indicates that user `mason` will log in on host `jupiter`.

D

A user or group authenticated by a Windows domain. In this case, `Domain` specifies either the simple domain name (for individual users) or the fully qualified domain name (for groups).

For example: `D:sales\putman` indicates user `putman` will log in through Windows domain `sales`.

Once configured, individual Windows domain users can log in to Unisphere for VMAX using a simple username. For example, `putman`.

Group Windows domain users can log in to Unisphere using either a simple domain `name\group` name or a fully qualified domain `name\group` name.

V

A user or group authenticated by a virtualization domain. In this case, `Domain` specifies the virtualization domain name.

Domain

Within role definitions, IDs can be either fully qualified (as above), partially qualified, or unqualified.

When the `Domain` portion of the ID string is an asterisk (`*`), the asterisk is treated as a wildcard, meaning any host or domain.

Note

When configuring group access, the `Domain` portion of the ID must be fully qualified.

For example:

D:ENG\jones

Fully qualified path with a domain and username (for individual domain users).

D:ENG.xyz.com\ExampleGroup

Fully qualified domain name and group name (for domain groups).

D:*\jones

Partially qualified that matches username jones with any domain.

H:HOST\jones

Fully qualified path with a hostname and username.

H:*\jones

Partially qualified that matches username jones within any host.

jones

Unqualified username that matches any jones in any domain on any host.

Name

Specifies the username relative to that authority. It cannot be longer than 32 characters and spaces are allowed if delimited with quotes.

Usernames can be for individual users or user groups.

User authorization

User authorization restricts the management operations users can perform on an array.

By default, authorization is enforced within Unisphere for VMAX against the respective authorization rules database of a given array. This enforcement is done regardless of the authorization control setting (Enabled/Disabled) for that array. SYMCLI uses this authorization control state to determine enforcement of rules. Unisphere for VMAX always behaves as if symauth is enabled (exception is the Initial Setup User).

A user with Administrator or SecurityAdmin privileges can map individual users or groups of users to specific user roles. Roles determine what operations users can perform.

Authorization for the Initial Setup User

The authorizations on an array determine the privileges the Initial Setup User has on the array. The relationship between the Initial Setup User and authorizations is defined by:

- If authorization is enabled, authorization rules are always enforced. The Initial Setup User could be locked out if no authorization rule exists for the user.
- If authorization is disabled and there are no authorization rules on the array, the Initial Setup User is granted Admin privileges.
- If authorization is disabled and there are no Admin or SecurityAdmin authorization rules on the array, the Initial Setup User is granted Admin privileges. All other rules are enforced as defined.
- When authorization is disabled and Admin or SecurityAdmin authorization rules are defined on the array, if the Initial Setup User does NOT have an authorization rule explicitly defined, the Initial Setup User will have NO permissions. All other rules are enforced as defined.

Unisphere REST API

Before you can use the Unisphere REST API, you must assign user authorization for each storage array a user is permitted to access. Users can be assigned the following roles:

- Monitor
- StorageAdmin
- Admiistrator
- SecurityAdmin

These user roles are valid for the currently available REST resource methods (GET, POST, and DELETE). When they become available, only Admin and StorageAdmin roles are able to initiate PUT methods.

For information on how to assign user roles, see the *EMC Unisphere for VMAX Installation Guide* and Unisphere for VMAX online help.

Multiple authorization roles

A user or group can be assigned up to four authorization roles.

Lockbox

Unisphere for VMAX uses the Common Security Toolkit Standalone Lockbox to store and protect sensitive information.

The Lockbox is first created during installation. During installation, you can use either the default password, or a password you define.

⚠WARNING

Loss of the user-defined password can lead to situations where the data stored in the Lockbox is unrecoverable.

On every Unisphere for VMAX startup, the default password is derived from the Stable System Values (SSVs) of the host's execution environment. The default password is not accessible to EMC or customer staff.

When the Unisphere for VMAX is upgraded, product information in the existing Lockbox is automatically copied into the new Lockbox when the Lockbox is first accessed.

SSVs are host-dependent. Changes to hardware or software on a host may require an update of the SSVs. You must update the SSVs in the Lockbox whenever the host SSVs no longer match the values in the Lockbox, including when the:

- Host upgrade reaches a certain threshold
- Lockbox file is moved to another host

The Lockbox includes a CLI utility to reset the host system SSVs.

Unisphere for VMAX and CA server certificates

At installation, the installer generates and installs the self-signed server certificate used for HTTPS transport-level security.

You can replace this certificate with the one issued by a trusted third-party.

You need the keystore password to replace a certificate. The keystore password is generated during installation and is stored in the following file:

`<SMAS installation>/jboss/domain/configuration/host.xml`

where `<SMAS installation>` is the directory where SMAS is installed.

Open the file and search for `keystore alias="tomcat" key-password=`.

You must generate a new JKS key/trust store file with the server certificate alias “tomcat” and key/store password. The key/trust store must contain all CA certificates needed for full certificate trust chain verification.

For information on how to replace, list and delete certificates, see the *EMC Unisphere for VMAX Installation Guide*.

Certificate revocation list for X.509 certificate-based authentication

For Unisphere for VMAX installations with X.509 certificate-based authentication enabled, you may optionally configure a Certificate Revocation List (CRL) for greater

PKI security. The CRL can be replaced periodically, based on the PKI security requirements set by your enterprise.

Port usage

Unisphere for VMAX components use the following ports:

Component	Port
https	8443
CLI	CLI 9999 (bound to the localhost, and not remotely accessible)
Remoting	4447
postgresql	3324 (bound to the localhost, and not remotely accessible)

Link-and-launch security

Link-and-launch clients connect to Unisphere for VMAX using HTTPS. The client and Unisphere for VMAX are required to establish mutual trust. That is, the client side trusts that the server is authentic.

Note

Link-and-launch is unavailable if Unisphere for VMAX is installed with the X.509 certificate-based client authentication option.

The link-and-launch client (acting as SSL client) must establish trust either:

- Explicitly, importing the Unisphere for VMAX self-signed certificate into the client's trust store
- Implicitly, if the Unisphere for VMAX self-signed certificate (generated during installation) is replaced with a certificate issued by a mutually-trusted CA (a CA trusted by both Unisphere for VMAX and the link-and-launch client).

Trust with the client's launching application is established by explicit registration (by Admin/SecurityAdmin) of the link-and-launch client's ID.

The client must provide a valid username of the Unisphere for VMAX user in whose context the link-and-launch is performed. Once trust is established, a one-time password (token) is issued to trusted link-and-launch clients. The tokens are then exchanged as a means to provide single sign on into Unisphere for VMAX.

Note

Unisphere for VMAX supports link-and-launch only in the context of users with Admin, StorageAdmin, or Monitor roles.

When the transport is fully secured (by mutual trust establishment) and the user is validated (during initial registration connection), Unisphere for VMAX issues the client a one-time password (OTP).

In the request that follows, the client exchanges the OTP for a launch token. The exchange must take place within OTP's time-to-live of 10 minutes, otherwise the process (of OTP acquisition and OTP-to-token exchange) must be started over.

The token is valid only for a single launch-and-link until the Unisphere for VMAX server reboots.

Unisphere data security

You can export and import some Unisphere for VMAX configuration settings to conveniently configure multiple installations.

Exported settings are protected with a customer-defined, one-time password.

The password must be communicated out-of-band as necessary.

Security alert system

Users with Administrator or StorageAdmin privileges can configure Unisphere for VMAX to deliver alert notifications for SNMP, e-mail, and Syslog.

The steps to configure alerts, manage alert thresholds, and view alert-related information are described in the *EMC Unisphere for VMAX Installation Guide* and online help.

Session timeout

Unisphere for VMAX sessions time out after 8 hours of user inactivity.

The timeout interval is not configurable.

When timeouts occur, the user is logged out, but the user account is not locked.

Root access requirements

Unisphere for VMAX requires Root/Administrator access privileges for installation, deployment, and operations.

CHAPTER 6

SMI-S Provider

EMC SMI-S Provider supports the SNIA Storage Management Initiative (SMI), an ANSI standard for storage management. Solutions Enabler provides the interface between the SMI and arrays running HYPERMAX OS 5977 or higher.

This chapter contains the following topics:

SMI-S checklist

The following checklist summarizes the security-related tasks you should perform to improve the security of your deployment.

Table 10 SMI-S security configuration checklist

Purpose of activity	Task
User-based access control	
Restrict user access to specific functionality.	Configure user authentication, create cstadmin and cstuser accounts, and map users to roles.
Log files and settings	
Administer SMI-S log files.	Display SMI-S log files.
Securely deploy SMI-S	
Enable authentication.	Enable authentication for CIM and non-CIM requests.
Create the Lockbox	
Create a Lockbox to store and protect sensitive information.	Create the CST Lockbox.

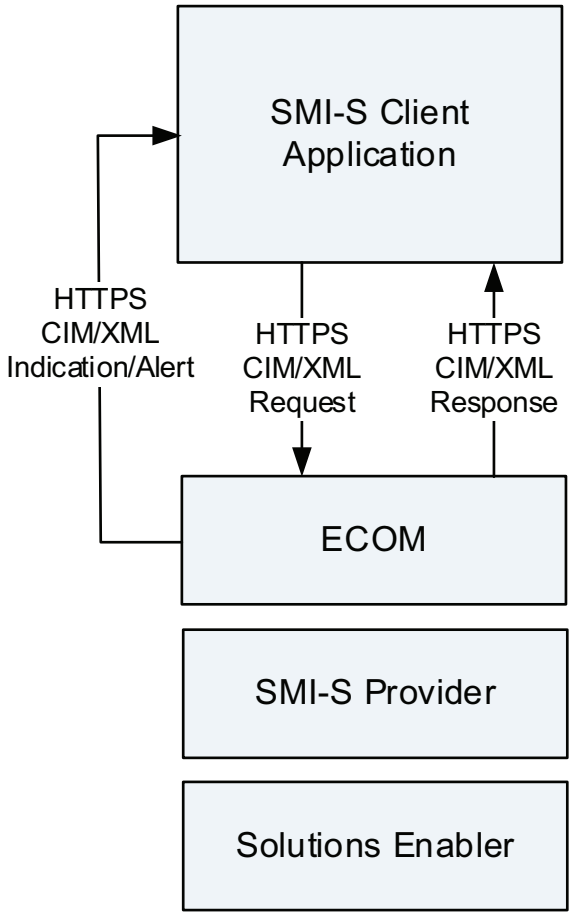
ECOM toolkit

SMI-S uses the EMC Common Object Manager (ECOM) Toolkit to implement security at a variety of levels. ECOM uses SSL and TLS protocols to secure and protect network requests, responses, and indication deliveries. Refer to the *EMC Common Object Manager (ECOM) Toolkit Deployment and Configuration Guide* for information about:

- ECOM port security
- Securing ECOM communication

Security controls map

Figure 4 SMI-S managed objects



User-based access control

This section describes user authorization, user authentication, and administrator user account.

User authorization

User access control to the SMI provider is provided by the ECOM authorization and security toolkit.

The ECOM login page can be accessed at `https://{hostname}:5989/ecomconfig`.

The default login credentials are

username: admin
password: #1Password

User authentication

ECOM supports three types of authorities: LocalDirectory (default), LDAP, and OSLogin. These authorities grant the user access.

To authenticate, ECOM requires user information following one of these two formats along with the user password:

```
user information := [ authority '/' ] [ domain '\' ] < username >
```

or

```
user information := [ domain '\' ] < username > [ '@' authority ]
```

If the authority recognizes the user, the authentication succeeds and ECOM returns a valid security token.

Configure authentication

The default authority is LocalDirectory. LocalDirectory is if the authority information is not informed by the user.

You can specify the Local Directory Authority as any substring from the Local Directory name as defined in Config.xml configuration file (default is LocalDirectoryTest). For example:

```
admin
LocalDir/admin
LocalDirectory/admin
LocalDirectoryTest/admin
admin@LocalDir
admin@LocalDirectory
admin@LocalDirectoryTest
```

LDAP servers can also be used as the authority to authenticate a user. For example:

```
PSO-AD-Authority/admin
PSO-SunOneAuthority/lennon
admin@PSO-AD-Authority
lennon@PSO-SunOneAuthority
```

Windows users can also be authenticated by the OSLogin authority.

The string "OSLogin" is used as the authority name in order to authenticate OS users.

Both local and domain users can be authenticated:

- If no domain is specified, the user is treated as a "local user" (default).
- If the domain is explicitly specified, the user is treated as a "domain user".

Both the fully-qualified domain name (FQDN) and the domain name can be used during authentication. The user-supplied domain entry will be converted into the FQDN.

For example:

```
OSLogin/Administrator
Administrator@OSLogin
OSLogin/CORP\mccartney
CORP\mccartney@OSLogin
OSLogin/corp.localdomain\ringo
corp.localdomain\ringo@OSLogin
```

Administrator user account

ECOM requires a user account under LocalDirectory authority named administrator.

This section describes the commands to create the administrator role, create a user, and assign the user to the role.

Create a cstadmin role

Use the `cstadmin create-role` command to create a new role.

The syntax for the `cstadmin create-role` command:

```
cstadmin create-role <role>
   -app=<app>
   -cstdir=<directory>
   -description <description>
   -passphrase=<passphrase>
```

<role>

(mandatory) Name of the role to create.

-app=*<app>*

(optional) Name of the application bootstrap file.

-cstdir=*<directory>*

(optional) Path to the CST configuration directory.

-description*<description>*

(optional) Description for the role.

-threshold

(optional) - Sets the Lockbox SSV threshold.

-passphrase=*<passphrase>*

(optional) - Passphrase for the Lockbox.

For example:

```
$ cstadmin create-role administrator -cstdir=.
Enter lockbox passphrase:
Confirm passphrase:
cstadmin: Role administrator created in role database
RoleManagement.
```

Create a cstadmin user

Use the `cstadmin create-user` command to create a local directory user account.

The syntax for the `cstadmin create-user` command:

```
cstadmin create-user <account>
   -app=<app>
   -cstdir=<directory>
   -description <description>
   -passphrase=<passphrase>
   -password=<initial password>
```

<account>

(mandatory) - Name of the local directory account to create.

-app=*<App>*

(optional) - Name of the application bootstrap file.

-cstdir=*<directory>*

(optional) - Path to the CST configuration directory.

-description*<description>*

(optional) - Description for the user.

-passphrase=*<passphrase>*

(optional) - Passphrase for the Lockbox.

-password=*<initial password>*

(optional) - Initial password for the account.

For example:

```
$ cstadmin create-user lennon -cstdir=c:/cst/lockbox
Enter new user's password:
Confirm passphrase:
Enter lockbox passphrase
cstadmin: User lennon created with account manager
LocalDirectoryTest.
```

Create a role mapping

Use the `cstadmin add-rolemember` command to add an identity to a role.

The syntax for the `cstadmin add-rolemember` command:

```
cstadmin add-rolemember <authority type>
   <authority type>
   <authority name>
   <account name>
   <role name>
   -app=<app>
   -cstdir=<directory>
   -group
  -passphrase=<passphrase>
```

<authority type>

Type of authority.

<authority name>

Name of authority.

<account name>

The account name to add.

<role name>

Role name to add.

-app=*<app>*

(optional) - Name of the application bootstrap file.

`-cstdir=`***<directory>***

(optional) - Path to the CST configuration directory.

-passphrase=*<passphrase>*

(optional) Passphrase for the Lockbox.

For example:

```
$ cstadmin add-rolemember LocalDirectory LocalDirectoryTest lennon
administrator -cstdir=c:/cst/lockbox
Enter lockbox passphrase
cstadmin: Role administrator added to lennon from account
manager
LocalDirectoryTest.
```

Component access control

Access control for SMI-provider components is provided by EMC Common Object Manager (ECOM).

EMC Common Object Manager (ECOM) Toolkit Deployment and Configuration Guide describes the steps to complete this task.

Log files and settings

If `SecurityLoggingEnabled` is set to true in the `Security_settings.xml` configuration file (located at *<ECOM_install_dir>*`/conf/`), ECOM logs security-related information to the file `securitylog.txt`.

Whether security logging is enabled or not, security-related information is always logged to the file `cimomlog.txt`.

`cimomlog.txt` and `securitylog.txt` are located at:

<ECOM_install_dir>`/log/`

Displaying log files

Use the ECOM web server to administer logs and security. The server can be accessed from:

`https://`*<ManagementIPAddress>*`:`*<port>*`/ecomconfig`

where *<port>* is a secure port as defined in `Port_settings.xml`.

EMC Common Object Manager (ECOM) Toolkit Deployment and Configuration Guide describes the steps to complete this task.

Port usage

Table 11 Ports used by SMI-S

Component	Service	Protocol	Port	Description
CIMXMLAdapter	ECOM	CIM/XML	5989	Secure HTTPS CIM/XML
WSManProtocol Adapte	ECOM	WS-MAN	5986	Secure HTTPS WS-MAN
EDAAAdapter	ECOM	Rest	5989	Secure HTTPS EDAA Rest

Network encryption

RSA BSAFE® library is included in all ECOM distributions to support SSL.

ECOM's secure communication capabilities are configured in the file `Security_settings.xml` located at *<ECOM_install_dir>*`/conf/`.

The relevant parameter settings in the file are:

CertificatesDirectory
The relative path to ECOM SSL certificates directory from *<ECOM_install_dir>*. Default: `conf/ssl`.

SSLCertFile
SSL certificate file name in `CertificatesDirectory`. Default: ecomtls.crt.

SSLKeyFile
SSL private key file name in `CertificatesDirectory`. Default: ecomtls.pk.

SSLCAFile
CA file name in `CertificatesDirectory`, needed if `SSLClientAuthentication` is enabled. Default: ecomtls.ca.

SSLClientAuthentication
Option that controls if the client SSL certificate should be verified or not.

SSLProtocol
Option that controls the method functions used to specify the various protocols supported by TLS and SSL connections for both the client and the server.

SSLCipherSuite
Option that controls the supported cipher suites of the SSL connection.

Group Replication

The EMC SMI-S Provider supports the SNIA SMI-S Replication Service profile. The Replication Services profile offers client applications the ability to manage replication using groups, also known as Group Replication. The Solutions Enabler global name service (GNS) can be started in Global Mode which will store the replication group

information into the HYPERMAX OS system. The advantage to storing replication group information in the storage array is that it centralizes the group data and makes it accessible to different hosts/servers accessing the same system.

The default installation of Solutions Enabler with SMI-S has the default GNS in Local Mode. In this mode, the replication group information is stored on the host running the Solutions Enabler SMI-S service.

Enabling Global Mode

Before you begin

These steps must be completed before any replication group operations are initiated.

Procedure

1. Shut down ECOM service.
2. Shut down Solutions Enabler daemons.
3. In the `SYMAPI/config/options` file add or enable the SYMAPI_USE_GNS = ENABLE option.
4. Start ECOM service. ECOM service will automatically start the Solutions Enabler daemons.

Enable authentication for SMI-S

To enable authentication for:

- CIM requests - set the configuration parameter `CIMRequest_AuthenticationEnabled` to true.
- non CIM requests - set `NonCIMRequest_AuthenticationEnabled`.

Manage the Lockbox

SMI-S uses a Lockbox to store and protect sensitive information.

The Lockbox must be initialized with a user account created and mapped to the administrator role.

The Lockbox must be located at *<ECOM_install_dir>*`/conf/cst/`.

Create the CST Lockbox

Use the `cstadmin initialize` command to create the Lockbox in the specified directory.

The command creates a new Lockbox in the specified directory used to store keys, signed configuration files and signatures.

The syntax for the cstadmin initialize command:

```
cstadmin initialize <directory>
   -attended
   -overwrite
   -set-lockbox-policy
   -threshold
   -two-factor
```

<directory>

(mandatory) - Path to CST configuration directory. Contains CSTconfiguration files. The Lockbox will be created in this directory.

-attended

(optional) - Attended Lockbox.

-overwrite

(optional) - Overwrites existing Lockbox.

-set-lockbox-policy

(optional) - Sets Lockbox passphrase policy.

-threshold

(optional) - Sets the Lockbox SSV threshold.

-two-factor

(optional) - Two factor Lockbox.

For example:

```
$ cstadmin initialize c:/cst/lockbox
Enter lockbox passphrase:
Confirm passphrase:
cstadmin: Lockbox c:\cst\lockbox\csp.clb initialized.
```

Security alerts

SMI Provider manages alerts as follows:

- SMI Provider registers to receive all Solutions Enabler storage-related events from Solutions Enabler.
- SMI Provider converts the storage-related events to indication objects.
- The indication objects are sent to ECOM indication handler, which then delivers the objects to listening client applications.

CHAPTER 7

Container Applications

Application containers are virtual machines that provide embedded applications on the storage array. This chapter contains the following topics:

Overview of container applications

The HYPERMAX OS converged operating system provides an open application platform for running data services. HYPERMAX OS includes a light-weight hypervisor that enables multiple operating environments to run as virtual machines on the storage array.

Application containers are virtual machines that provide embedded applications on the storage array. Each container virtualizes hardware resources required by the embedded application, including:

- Hardware needed to run the software and embedded application (processor, memory, PCI devices, power management)
- VM ports, to which LUNs are provisioned
- Access to necessary drives (boot, root, swap, persist, shared)

Embedded NAS (eNAS) is a data service offered as a container application. eNAS enables consolidated block and file storage without the expense and complexity of gateway hardware.

Embedded Management (eManagement) is a container application that allows you to manage arrays running HYPERMAX OS without requiring a dedicated management host.

Container applications are installed at the factory. No additional security procedures are required.

Container application access IDs

The access ID for a container application is a shared secret between Solutions Enabler and HYPERMAX OS. Solutions Enabler generates the access ID based on the type of container application during first boot.

When a container application issues a syscall, HYPERMAX OS validates the access ID, and associates the privilege check with the appropriate group.

Container application access IDs have the following characteristics:

- Traditional access IDs (generated using attributes of the hardware), are not valid for container applications.
- The shared secret is not visible through any interface.
- Customers cannot disable alternate access ID mode or change the access ID.

Client/server mode

By default, client/server mode operations use the access ID of the server. Access control checks are performed against the rules established for the server host.

Customers may prefer to apply client host privileges rather than those of the host.

To change the access control privileges to the client, perform the following:

- On the client host:
  Set the SYMAPI option SYMAPI_CLIENT_SIDE_ACCESS_ID to ENABLE

  ```
  symcli -option set SYMAPI_USE_ACCESS_ID -value CLIENT
  ```

  This tells SYMAPI to send the client access ID to the server.

- On the server host:
  Set the SYMAPI option SYMAPI_USE_ACCESS_ID to CLIENT or ANY.

  CLIENT - (default value) The server expects all clients to send their access IDs. The server will never use the container application access ID.

  ANY - If the client sends an access ID, the server uses it. If the client does not send an access ID, the server uses the container application access ID.

Customers may change the server side setting using vApp Manager.

Note

Admin privileges on each host are required to modify access for that host.

CHAPTER 8

Embedded NAS

This chapter provides information on the security configuration required for embedded NAS (eNAS), an embedded application available on storage arrays running HYPERMAX OS. Topics include:

Embedded NAS

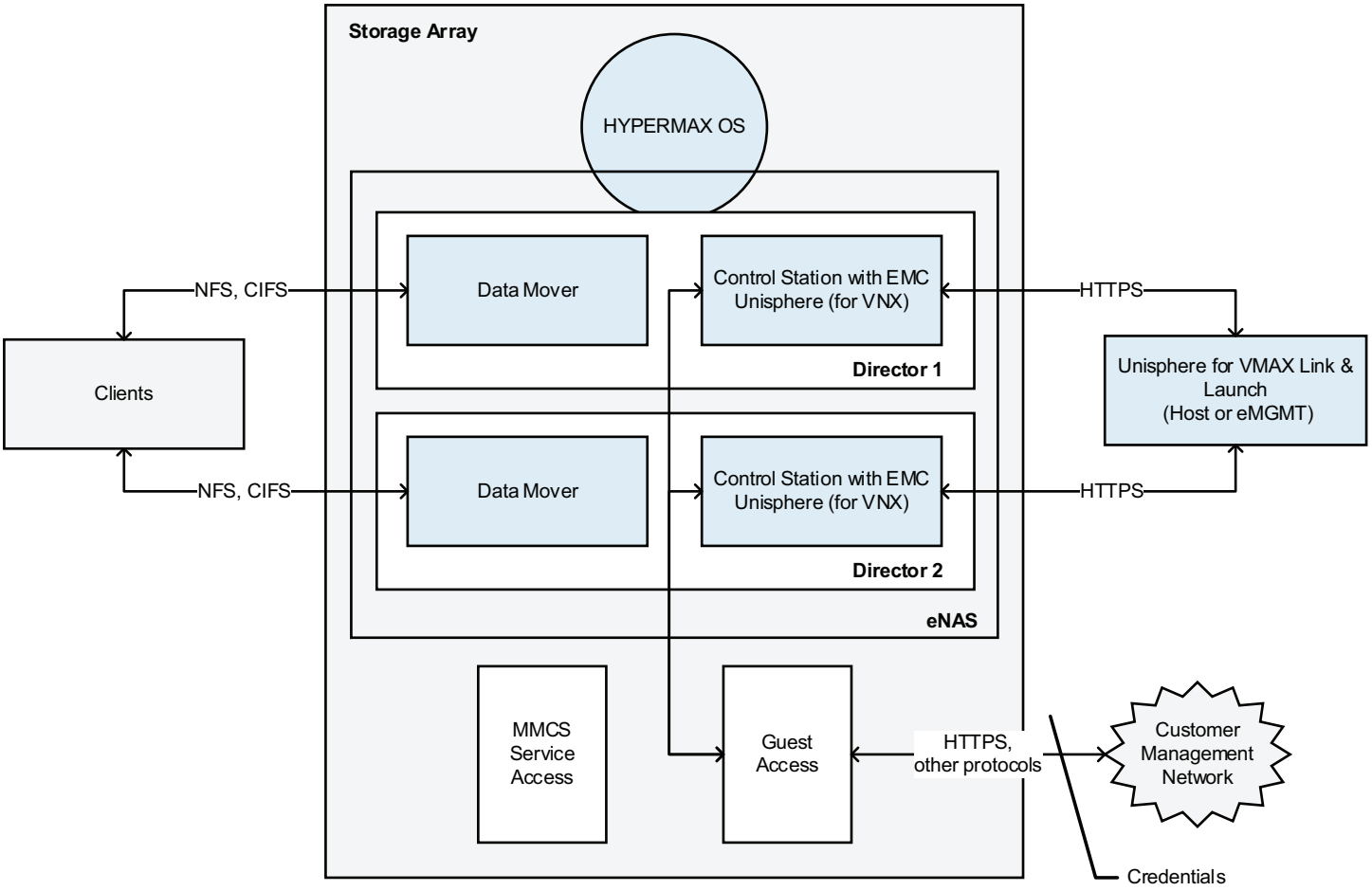
Embedded NAS (eNAS) uses the lightweight hypervisor provided in HYPERMAX OS to create and run a set of virtual machines on storage array controllers. These virtual machines host two major elements of eNAS: software data movers and control stations. These virtual machines are distributed based on the mirrored pair architecture of the storage array to evenly consume resources for both performance and capacity. All block and file resources are managed through the intuitive, easy to use Unisphere for VNX management interface.

eNAS extends the value of storage arrays running HYPERMAX OS to file storage by enabling customers to leverage vital enterprise features including SLO-based provisioning, Host I/O Limits, and FAST technologies for both block and file storage.

The eNAS guest runs in a virtual environment created by a “container”. Containers identify the resources (memory, ports, and LUNs) used by their guest. When a guest is created, HYPERMAX OS assigns an internal IP address that is not exposed to the customer network. MAC Address filtering prevents unauthorized access between guests on the array's internal network.

Security controls map

Figure 5 Embedded NAS managed objects



The security features and tasks the eNAS guest running on the storage array running HYPERMAX OS are the same as those for the VNX series.

- *EMC VNX Series Security Configuration Guide for VNX* provides information on the following security-related topics:
  - Access control
  - Logging
  - Communication security
  - Data security settings
  - Security maintenance
  - Advanced management
- *EMC VNX Series Command Line Interface Reference for File* provides information the CLI commands to manage access control, certificates, LDAP configuration, and other security-related activities.

⚠ CAUTION

Customers are responsible for securing their eNAS/VNX deployment. Pre-configured settings may not be sufficiently secure for their needs. *EMC VNX Series Security Configuration Guide for VNX* provides additional information.

CHAPTER 9

Embedded Management

This chapter provides information on the security configuration required for embedded management (eMgmt). eMgmt enables you to manage an array running HYPERMAX OS without software installed on a host. Topics include:

Embedded management

Embedded management (eManagement) embeds management software (Solutions Enabler, SMI-S, Unisphere for VMAX) on the storage array, enabling customers to manage the array without software installed on a host.

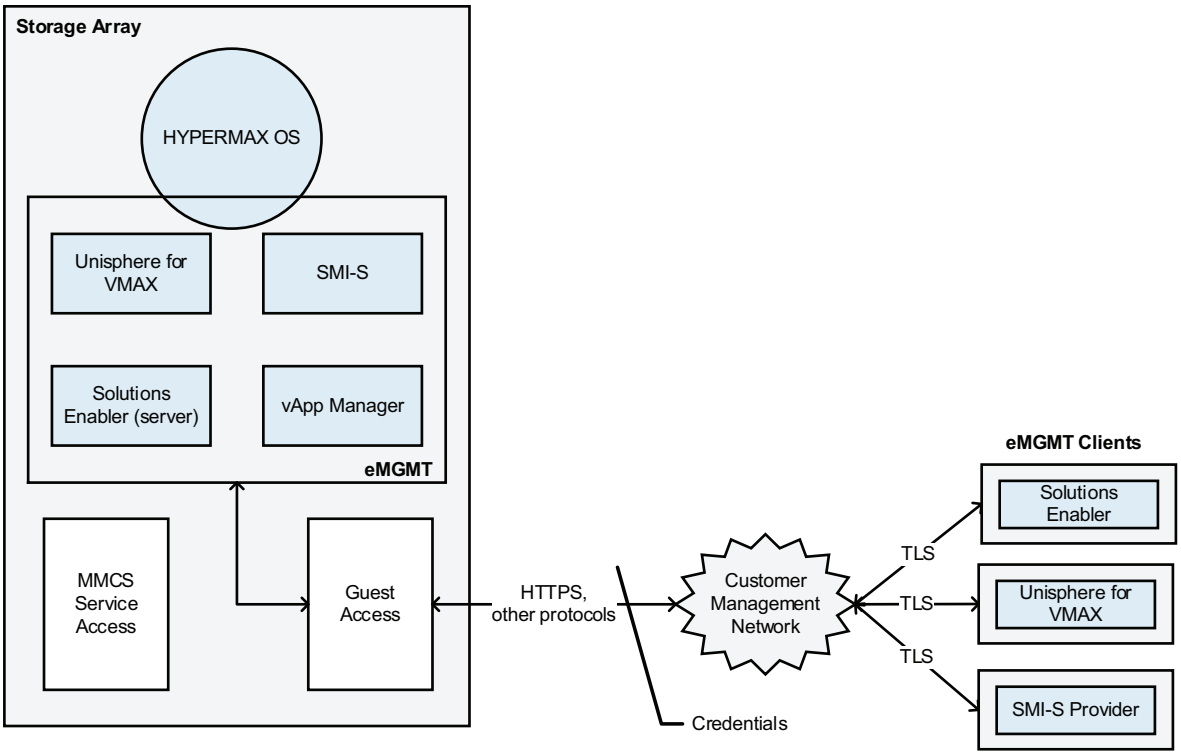
Note

eManagement manages a single storage array running HYPERMAX OS and any SRDF attached arrays. Customers with multiple storage arrays who want a single control pane can use the traditional host-based management interfaces.

eManagement is enabled at the EMC factory.

Security controls map

Figure 6 eManagement managed objects



Note

MMCS service access and guest access to the array are distinct and separate operations. Service users do not have access to any traffic on the guest interface.

Virtual Machine ports

Virtual machine (VM) ports are associated with virtual machines to avoid contention with physical connectivity. VM ports are addressed as ports 32-63 per director FA emulation.

LUNs are provisioned on VM ports using the same methods as provisioning physical ports.

A VM port can be mapped to one and only one VM.

A VM can be mapped to more than one port.

CHAPTER 10

vApps

This chapter contains the following topics:

vApp overview

EMC delivers virtual appliances (vApps) for:

- Unisphere for VMAX
- Solutions Enabler
- SMI-S
- VASA Provider
  The VASA Provider orchestrates the lifecycle of Virtual Volumes (VVols) and their derivatives: snapshots, clones, and fast-clones. It also provides storage topology, capabilities and status information to the vCenter ™ and the ESXi hosts.

vApp checklist

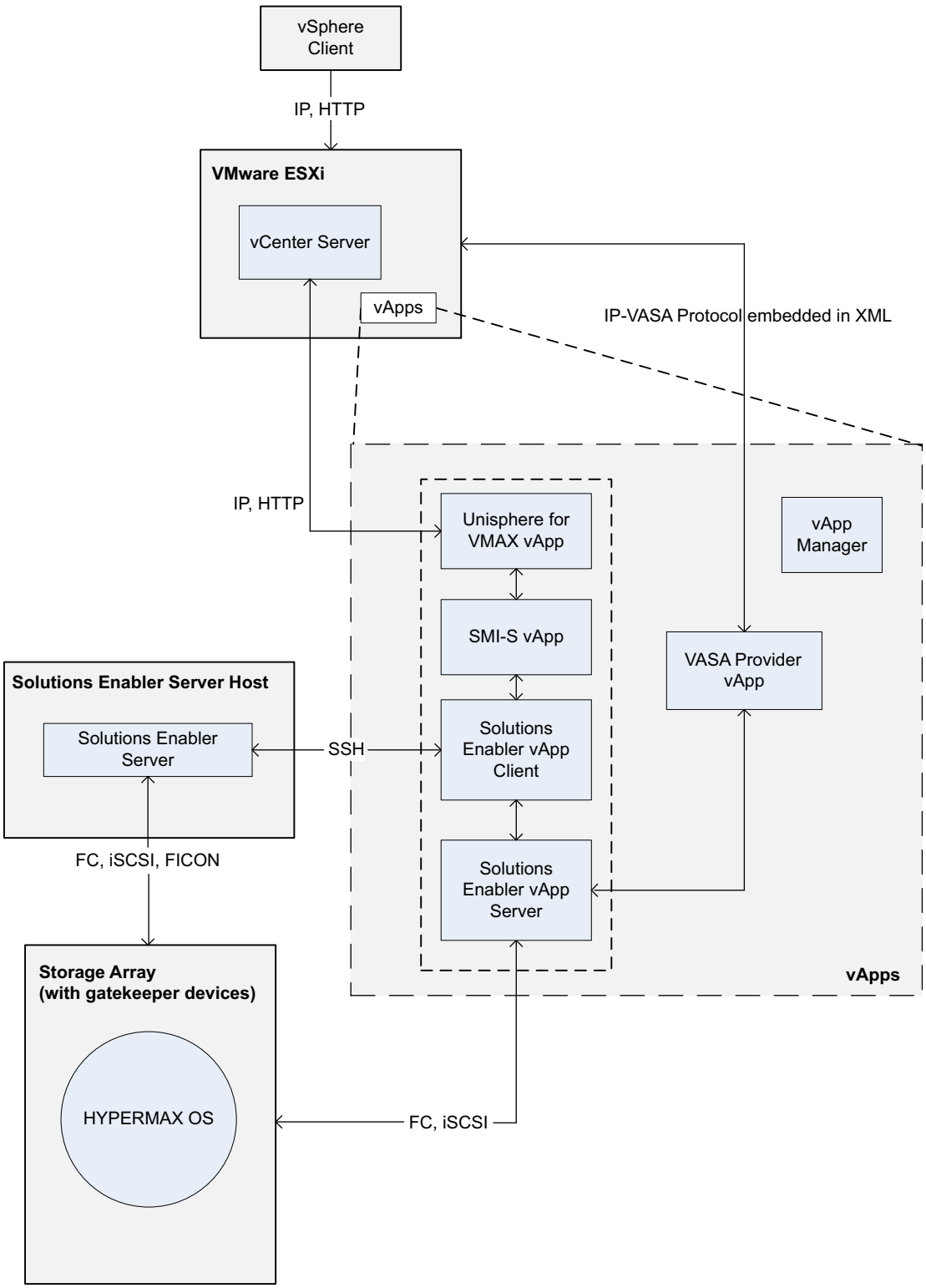
The following checklist summarizes security-related tasks you should perform to improve the security of your deployment.

Table 12 vApp security configuration checklist

Purpose of activity	Task
User-based access control: Manage user accounts	Manage user authentication
Log files and settings: Manage log files	Download log files
Certificate files: Replace generated certificates with customer-supplied (trusted) certificates for secure communications	Replace pre-generated SSL certificates
Security settings: Perform anti-virus scans, download scan logs, and edit the anti-virus configuration file	Manage Clam anti-virus

Security controls map

Figure 7 vApp managed objects



Deployment settings and points of access

Each vApp is installed from a single Open Virtualization Format (OVF) archive and deployed in a standard ESXi appliance.

There are three points of access:

- vApp Manager
- SSH
- VM console

vApps are designed to be managed by the vApp Manager. There is no direct user access except when SSH is explicitly enabled for troubleshooting. No components can be individually managed.

vApp Manager
vApp Manager is a browser-based graphical user interface console contained within each vApp that allows you to perform management and configuration tasks for the vApp. vApp manager is the sole management interface for accessing vApps and is accessed via a secure https layer. For example:

```
https://hostname:5480
```

SSH
You can enable the SSH port for an SSH session to troubleshoot the appliance or storage system. The default state of the SSH port is disabled.

You must log in to the vApp Manager to enable or disable the SSH port. Authentication is required for login.

⚠ CAUTION

Troubleshooting the appliance or storage system should only be done under the direction of EMC Customer Support.

Virtual machine console
You can access the virtual machine console via the ESXi server. The following activities are supported through ESXi server access:

- Network configuration
- Upgrades
- Setting timezones

Limiting access to management interfaces

You can limit access to management interfaces from a defined list of hosts. In vApp Manager, you can specify an IP/Host name to restrict the vApp client access to only that domain. Both the server and client components must be part of the same network.

For information on how to change the domain name, see the vApp Manager online help.

User authentication

vApp Manager users can:

- Configure the Common Security Toolkit Lockbox
- Configure and update vApp options
- Retrieve log files

The vApp Manager provides two types of user authentication:

- Local directory authentication (username and password)
- Lightweight Directory Access Protocol (LDAP) authentication

LDAP allows for distributed directory information services over a network of hosts. A client must provide a set of parameters to configure LDAP, which then allows connection to the LDAP server, and secures communication between hosts on the network.

You can add new local users or map existing LDAP users. New users are assigned one of two roles:

- admin
- service

The default role is admin.

LDAP admin users can be either a "user" or "group" type. All users belonging to an LDAP group can perform all vApp Manager operations.

The vApp Manager contains online help that describes the steps to manage user authentication, including:

- Configuring LDAP
- Changing the LDAP configuration
- Importing certificates
- Adding user accounts
- Removing user accounts
- Changing user passwords

VASA Provider authentication

Authentication and authorization between vCenter and the VASA Provider is achieved by registering the VASA Provider in the vSphere Web Client for vCenter. For information on registering the VASA Provider, see the *EMC VMAX VASA Provider Release Notes*. It is recommended that you change the default password for security.

After the VASA Provider is registered, certificates are the authorization mechanism. The certificate authorities can be owned by VMware Certificate Authority (VMCA), EMC or a third party.

Default user accounts

vApp Manager has one or two default user accounts.

A default user account is created during installation. The default user account cannot be removed.

vApp default user accounts are:

Table 13 vApp default accounts

vApp	Username	Password
Unisphere for VMAX	seconfig	seconfig
Solutions Enabler	seconfig	seconfig
VASA Provider	vpconfig	vpconfig

The first time you log in you will be prompted to change the password for the default user account. You can subsequently change the password at any time.

A second default user account is created if you enable SSH. The default SSH user account for all vApps is:

username: cseadmin
password: cseadmin

You can change the password for the default SSH account at any time.

Port usage

vApp Manager uses the ports listed in the following table. All other ports are blocked.

Table 14 Network ports used in vApps

Component	Protocol	Port	Description
SSH	TCP	22	SSH port. This port can be enabled/ disabled using vApp Manager. Default: disabled.
Solutions Enabler	TCP	2707	Standard EMC Solutions Enabler server port for client-server communication.
vApp Manager	TCP	5480	Port where the vApp JBoss web server listens for vApp manager requests. Listening port for uploading certificates and licenses to Unisphere for VMAX vApp Manager over HTTP.
SMI	TCP	5988, 5989	Standard EMC SMI port.
VASA Provider	TCP	5989	Standard EMC secure port. VASA Provider does not conflict with SMI-S port usage since

Table 14 Network ports used in vApps (continued)

Component	Protocol	Port	Description
			the vApps are installed in separate OVF packages.
vApp for Unisphere for VMAX	TCP	8443	Standard EMC Unisphere for VMAX listening port.

Log files and settings

You can use the vApp Manager to download the following log files from the vApp:

- Daemon log files, including:
  - storapid
  - storgnsd
  - storrdfd
  - storevntd
  - storsrmd
  - storwatchd
  - storstpd
  - storsrvd
  - ecom
  - univmax
- Appliance (vApp Manager) log files
- First level log files and other diagnostic information obtained by the EMCGrab utility

The vApp Manager online help describes the steps to download log files.

VASA Provider Log Files

The VASA Provider log files are located in `/opt/emc/vvol/log`.

The log files are:

- HTTP_trace.log
- VVolProvider-<date>.log cimomlog.txt
- udb.log
- vp.log
- securitylog.txt

Log file management

Logging levels, log file retention, and synchronization between the log files and the ESX timer are not configurable.

Log file entries cannot be streamed to an external log service, such as syslog.

If the disk space utilized by log files reaches 80% capacity, an alert is generated. This threshold is not configurable.

SSL certificates

SSL certificates for the vApp Manager can not be modified.

You can use the vApp Manager to import an alternate (custom) SSL certificate for the `storsrvd` daemon. The vApp Manager online help describes the steps to create and update SSL certificates.

The certificate is used when `stordaemon` command requests are made from a remote client. Certificates can be self-signed or CA-signed.

Importing an alternate certificate for the `storsrvd` daemon requires the following files:

- Private key file
- Replacement certificate file
- Trust certificate file

These files must be in a .pem format. For example:

```
customer_key.pem
```

The common name (CN) of the certificate must include `storsrvd` followed by a space, and the fully qualified name of the host where the certificate will be installed. For example:

```
storsrvd my.host.com
```

Data security settings

The vApp Manager persistent data files include the following appliance configuration files:

- Daemon Option file
- Option file
- Network configuration file
- symapi.db file
- daemon specific files

To download the persistent files using vApp Manager, click the **Download Persistent Data** button on the **Appliance Data/Log** tab.

Downloaded data files are saved to a `.zip` file (including a `.gpg` file) named:

```
product-name_export_persistenent_data_date_time.zip
```

The data is fully encrypted. The encryption key is not configurable and cannot be modified.

Starting in Solutions Enabler 8.0.2, vApp Manager verifies that there is sufficient space to create the `.zip` file. If there is not sufficient space, a message similar to the following is displayed:

```
Insufficient space to compress persistent data. Please try
cleaning up temporary files.
```

You can click the **CLEAR FILES** button to create sufficient space to complete the compression and download.

Note

In Unisphere for VMAX deployments, you need to stop and restart SMAS in order to clear the files. The steps to start and stop SMAS are described in the *EMC Unisphere for VMAX Installation Guide*.

Serviceability

There is no special login to vApp Manager for service personnel.

EMC Service Personnel may ask you to enable SSH access for troubleshooting the vApp. Ensure SSH is disabled except upon request from EMC.

Security patches and other updates are applied by upgrading the vApp installation image from the virtual machine console.

Alerts

vApp Manager has two pop-up alerts:

- Virus update alert - Displayed when an update for ClamAV is available. ClamAV is an anti-virus package that detects viruses, trojans, malware, and other malicious threats.
- Log file usage alert - Displayed when a log file reaches 80% of available capacity.

These alerts are display-only. They are not forwarded to an alert notification manager.

Clam anti-virus

The vApp Manager is packaged with Clam Anit-virus (ClamAV), an open source (GPL) anti-virus capability designed to detect viruses, trojans, malware, and other malicious threats on the appliance virtual machine. ClamAV supports on-demand scanning, anti-virus updates, access to scan log files, and editing the ClamAV configuration file.

Information on managing ClamAV is included in the vApp Manager online help.

Upgrades

Updates to vApp are installed using a full ISO upgrade.

Patching is not supported.

CHAPTER 11

Snapshots

TimeFinder SnapVX delivers point-in-time copies of volumes and snapshots of Storage Groups. Secure snaps provide added security by preventing accidental deletion of snapshot data.

This chapter contains the following topics:

TimeFinder SnapVX

EMC TimeFinder SnapVX creates and manages point-in-time snapshots of critical data that can be used for backups, decision support, and to refresh data warehouse, test, and development environments. SnapVX snapshots do not require target volumes. SnapVX snapshots share back-end allocations with the source volume and other snapshots on the source volume.

TimeFinder SnapVX is supported on VMAX arrays running HYPERMAX OS 5977 and higher, and snapshots are always consistent. Consistency across multiple arrays is achieved when source devices are in a composite group.

Secure snaps

Introduced with HYPERMAX OS 5977 Q2 2017 SR, secure snaps is an enhancement to the current snapshot technology. Secure snaps prevent administrators or other high-level users from intentionally or unintentionally deleting snapshot data. In addition, Secure snaps are also immune to automatic failure resulting from running out of Storage Recourse Pool (SRP) or Replication Data Pointer (RDP) space on the array.

When creating a secure snapshot, you assign it an expiration date/time either as a delta from the current date or as an absolute date. Once the expiration date passes, and if the snapshot has no links, HYPERMAX OS automatically deletes the snapshot. Prior to its expiration, Administrators can only extend the expiration date - they cannot shorten the date or delete the snapshot. If a secure snapshot expires, and it has a volume linked to it, or an active restore session, the snapshot is not deleted; however, it is no longer considered secure.

Note

Secure snapshots may only be terminated after they expire or by customer-authorized EMC support. Refer to Knowledgebase article 498316 for additional information.

CHAPTER 12

Data at Rest Encryption

This chapter contains the following topics:

Overview

Data at Rest Encryption (D@RE) provides hardware-based, on-array, back-end encryption for VMAX storage arrays running HYPERMAX OS 5977.596.583 or higher. Back-end encryption protects your information from unauthorized access when drives are removed from the system. D@RE provides encryption on the back end using SAS I/O modules that incorporate AES-XTS data-at-rest encryption, designed to be FIPS 140-2 Level 1 compliant. These modules encrypt and decrypt data as it is being written to or read from a drive. Both HDDs and SSDs are protected and all configured drives are encrypted, including both RAID groups and spares. In addition, all array Vault contents are encrypted.

D@RE can use either of the following methods for key management:

- D@RE can use its RSA® Embedded Key Manager
- You can configure D@RE to interface with an OASIS Key Management Interoperability Protocol (KMIP) compliant external key manager

D@RE keys are self-managed, and there is no need to replicate keys across volume snapshots or remote sites. The key manager provides a separate, unique DEK for all drives in the array including spare drives.

By securing data on enterprise storage, D@RE ensures that the potential exposure of sensitive data on discarded, misplaced, or stolen media is reduced or eliminated. As long as the key used to encrypt the data is secured, encrypted data cannot be read. In addition to protecting against threats related to physical removal of media, this also means that media can readily be repurposed by destroying the encryption key used for securing the data previously stored on that media.

D@RE is compatible with all VMAX3 and VMAX All Flash system features, allows for encryption of any supported logical drive types or volume emulations, and delivers powerful encryption without performance degradation or disruption to existing applications or infrastructure.

D@RE protects against unauthorized data access when drives are lost, failed or stolen. Features include:

- Secure replacement for failed drives that cannot be overwritten. Delete the applicable keys, and the data on the failed drive is unreadable.
- Protection against stolen drives. When a drive is removed from the array, the key stays behind, making data on the drive unreadable.
- Faster drive sparing. The drive replacement script crypto-shreds data by destroying the keys associated with the removed drive.
- Secure array retirement. Simply delete all copies of keys on the array, and all remaining data is unreadable.
- All configured drives are encrypted, including RAID groups and spares.
- PowerVault data is encrypted on Flash I/O modules (instead of drives).
- You can use the SYMCLI (symcfg list -v), Unisphere for VMAX (icon on the front panel), vApp Manager, and SMI-S to display whether D@RE is enabled on a storage array.

D@RE is a licensed feature. For new systems, D@RE is pre-configured and installed at the factory. If you are using the embedded key manager, no user management of D@RE's security features are required or possible. If you are using an external key manager, additional steps are required to connect to the key servers.

Note

If you have an existing storage array running HYPERMAX OS without D@RE enabled, you must upgrade to enable D@RE. The upgrade is disruptive and requires re-installing the array, and may involve a full data back up and restore. Before you upgrade, you must plan how to manage any data already on the array. EMC Professional Services offers services to help you upgrade to D@RE.

Key manager

D@RE provides enterprise-level key management using by integrating with a KMIP compliant external key manager. For a list of supported key managers, see E-Lab™ Interoperability Navigator (ELN) at https://elabnavigator.emc.com.

The key manager provides a separate, unique Data Encryption Key (DEK) for each disk in the array, including spare drives. As long as the key used to encrypt the data is secured, encrypted data cannot be read. When D@RE is enabled:

- The key manager generates a Key Encryption Key (KEK).
- When a RAID group or pool is configured, the key manager generates an encryption key (DEK) for each drive. Every drive has a unique key. When a drive is added or replaced, a new DEK is generated. After drive replacement, the old key is destroyed both in the array configuration and key manager.

DEKs and KEKs can only be used on the array where they are generated (embedded key manager) or requested from (KMIP compliant external key manager). DEKs are encrypted with a KEK and pushed from the Key Manager to the controller as necessary during normal operations, such as when a new drive is added.

When data requiring encryption is replicated to another array, D@RE must be enabled at both the primary and secondary sites. Drives at the primary site have different encryption keys to those at the secondary site.

The VMAX Audit Log records all key management events.

Key protection

The local keystore file is encrypted with a 256-bit AES key derived from a randomly-generated password, and stored in the Common Security Toolkit (CST) Lockbox which leverages RSA's BSAFE technology.

The Lockbox is protected using MMCS-specific stable system values of the primary MMCS. These are the same SSVs that protect Symmetrix Secure Credentials.

Compromising the MMCS's drive or copying Lockbox/keystore files off the array causes the SSV tests to fail.

Compromising the entire MMCS only gives an attacker access if they also successfully compromise Symmetrix Service Credentials (SSC).

There are no backdoor keys or passwords to bypass D@RE security.