

SANtricity ES Storage Manager V 10.80



BOSCH

en Initial Configuration and Software Installation

Table of Contents

1	Safety Precautions	6
1.1	Warning Notices	6
1.2	Caution Notices	9
2	General	11
3	Deciding on the Management Method	12
3.1	Key Terms	12
3.2	Procedure – Management Method	12
3.3	Things to Know – In-Band and Out-of-Band Requirements	15
4	Setting Up the Storage Array for Windows Server 2008 Server Core	17
4.1	Procedure – Configuring the Network Interfaces	17
4.2	Procedure – Setting the iSCSI Initiator Services	18
4.3	Procedure – Installing the Storage Management Software	18
4.4	Procedure – Configuring the iSCSI Ports	19
4.5	Procedure – Configuring and Viewing the Targets	19
4.6	Procedure – Establishing a Persistent Login to a Target	20
4.7	Procedure – Verifying Your iSCSI Configuration	20
4.8	Procedure – Reviewing Other Useful iSCSI Commands	21
4.9	Procedure – Configuring Your Storage Array	21
5	Installing the SANtricity ES Storage Manager Software	22
5.1	Key Terms	22
5.2	Things to Know – All Operating Systems	22
5.3	Things to Know – Specific Operating Systems	22
5.4	Things to Know – System Requirements	23
5.5	Procedure – Installing the SANtricity ES Storage Manager Software	25
5.6	Things to Know – Software Packages	25
5.7	Procedure – Manually Installing RDAC on the Linux OS	29
6	Configuring the Host Bus Adapters	30
6.1	Procedure – Configuring the HBAs	30
6.2	Things to Know – Changing to Linux Operating System Settings, Failover Driver Settings, and HBA Settings for DMMP31	
6.3	Things to Know – Changing the Linux Failover Driver and HBA Settings for MPP	33
6.4	Things to Know – Changing Windows FC and iSCSI HBA Settings	35
6.5	Things to Know – Changing the SAS Host Adapters	37
6.6	Things to Know – Changing the VMware OS HBA Settings	38
6.7	Things to Know – Changing the HP-UX OS for HBAs	39
7	Starting SANtricity ES Storage Manager	40
7.1	For Additional Information	40
7.2	Procedure – Starting SANtricity ES Storage Manager	40

7.3	Things to Know – Enterprise Management Window and Array Management Window	40
8	Adding the Storage Array	43
8.1	Things to Know – Storage Array	43
8.2	Procedure – Automatically Adding a Storage Array	43
8.3	Procedure – Manually Adding a Storage Array	43
8.4	Things to Know – Rescanning the Host for a New Storage Array	44
8.5	Procedure – Rescanning the Host for a New Storage Array	45
9	Naming the Storage Array	46
9.1	Things to Know – Naming the Storage Array	46
9.2	Procedure – Naming a Storage Array	46
10	Resolving Problems	47
10.1	Procedure – Resolving Problems	47
10.2	Retrieving Trace Buffers	47
11	Adding Controller Information for the Partially Managed Storage Array	49
11.1	Key Terms	49
11.2	Things to Know – Partially Managed Storage Arrays	49
11.3	Procedure – Automatically Adding a Partially Managed Storage Array	49
12	Manually Configuring the Controllers	51
12.1	Things to Know – Manually Configuring the Controllers	51
12.2	Things to Know – Options for Manually Configuring the Controllers	51
12.3	Procedure – Configuring the Management Station	52
12.4	Procedure – Configuring the Controllers	52
13	Setting a Password	55
13.1	Things to Know – Passwords	55
13.2	Procedure – Setting a Password	55
14	Removing a Storage Array	56
14.1	Things to Know – Removing Storage Arrays	56
14.2	Procedure – Removing a Storage Array	56
15	Configuring Email Alerts and SNMP Alerts	57
15.1	Key Terms	57
15.2	Things to Know – Alert Notifications	57
15.3	Procedure – Setting Alert Notifications	57
16	Changing the Cache Memory Settings	59
16.1	Key Terms	59
16.2	Things to Know – Cache Memory Settings	59
16.3	Procedure – Viewing the Cache Memory Size Information	59
16.4	Procedure – Changing the Cache Memory Settings	59

16.5	Procedure – Changing the Volume Cache Memory Settings	60
17	Enabling the Premium Features	61
17.1	Key Terms	61
17.2	Things to Know – Premium Features	61
17.3	Procedure – Enabling the Premium Features	61
18	Defining the Hosts	62
18.1	Things to Know – Hosts	62
18.2	Things to Know – Host Groups	62
18.3	Things to Know – Storage Partitions	62
18.4	Procedure – Defining the Hosts	65
18.5	Procedure – Defining the iSCSI Hosts	65
19	Configuring the Storage	66
19.1	Key Terms	66
19.2	Things to Know – Data Assurance	66
19.3	Things to Know – Allocating Capacity	67
19.4	Things to Know – Volume Groups and Volumes	68
19.5	Things to Know – Host-to-Volume Mappings and Storage Partitions	68
19.6	Things to Know – Hot Spare Drives	69
19.7	Things to Know – Full Disk Encryption	69
19.8	Procedure – Configuring the Storage	71
20	Downloading the Drive and ATA Translator Firmware for SATA Drives	73
20.1	Things to Know – A Preview of the Download Drive and ATA Translator Firmware Dialog	74
20.2	Procedure – Starting the Download Process	74
20.3	Procedure – Selecting the Drive and the ATA Translator Firmware	74
20.4	Procedure – Updating the Firmware	75
20.5	Procedure – Monitoring the Progress of the Download	75
21	Restrictions	77

1 Safety Precautions

Definitions of safety notices:

- WARNING indicates a potentially hazardous situation that could result in death or severe personal injury.
- CAUTION indicates a potentially hazardous situation that could result in moderate or minor personal injury.

1.1 Warning Notices

**WARNING!****Risk of electrical shock**

If there is evidence of fire, water, or structural damage, never turn on the power to the equipment.

**WARNING!****Risk of electrical shock**

Before removing or installing a power supply, turn off the power switch, and unplug the power cord.

**WARNING!****Risk of exposure to laser radiation**

Do not disassemble or remove any part of a Small Form-factor Pluggable (SFP) transceiver because you might be exposed to laser radiation.

**WARNING!****Risk of bodily injury**

The battery can weigh up to 10.9 kg (24 lb). When you remove the battery, be prepared to support its weight. If the battery is dropped, the impact might cause bodily injury, including deep puncture wounds caused by the battery pins.

**WARNING!****Risk of bodily injury**

If the bottom half of the cabinet is empty, do not install components in the top half of the cabinet. If the top half of the cabinet is too heavy for the bottom half, the cabinet might fall and cause bodily injury. Always install a component in the lowest available position in the cabinet.

**WARNING!****Risk of bodily injury**

Attach the stability foot before moving the cabinet. If you do not attach the stability foot, the cabinet might become unstable, or it might fall. This problem is most likely to occur when the cabinet is moved along inclined surfaces or over uneven surfaces.



WARNING!

Risk of bodily injury

Only move a populated cabinet with a forklift or adequate help from other persons. Always push the cabinet from the front to prevent it from falling over. A fully populated cabinet can weigh more than 909 kg (2000 lb). The cabinet is difficult to move, even on a flat surface. If you must move the cabinet along an inclined surface, remove the components from the top half of the cabinet, and make sure that you have adequate help.



WARNING!

Risk of bodily injury



>18 kg (39,7 lbs)

Two persons are required to safely lift the component.



WARNING!

Risk of bodily injury



>35 kg (70,5 lbs)

Three persons are required to safely lift the component.



WARNING!

Risk of bodily injury



>55 kg (121,2 lb)

Four or more persons are required to safely lift the component.

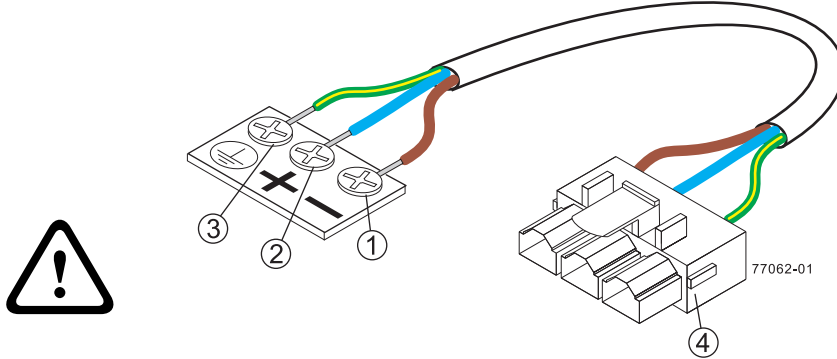


WARNING!

Risk of fire or chemical burn

Before disposing of a used battery, review the battery warning label. The label reads: The battery used in this device may present a risk of fire or chemical burn if mistreated. DO NOT disassemble, heat above 60°C (140°F), crush or puncture, short circuit external contacts, or dispose of in fire or water. Use LSI recommended charger only. Replace only with original LSI batteries.

WARNING!
Risk of electrical shock



- 1 - Supply (Negative), Brown Wire, -48 VDC
- 2 - Return (Positive), Blue Wire
- 3 - Ground, Green/Yellow Wire
- 4 - DC Power Connector

This unit has more than one power source. To remove all power from the unit, all DC MAINS must be disconnected by removing all power connectors (item 4 below) from the power supplies.

WARNING!
Risk of bodily injury



Only move a populated cabinet with a forklift or adequate help from other persons. Attach the stability foot before moving the cabinet. If you do not attach the stability foot, the cabinet might become unstable, or it might fall. Always push the cabinet from the front to prevent it from falling over.

A fully populated cabinet can weigh more than 636 kg (1420 lb). The cabinet is difficult to move, even on a flat surface. If you must move the cabinet along an inclined surface, remove the components from the top half of the cabinet, and make sure that you have adequate help.

WARNING!
Risk of bodily injury



A qualified service person is required to make the DC power connection according to NEC and CEC guidelines.

WARNING!
Risk of bodily injury



An empty tray weighs approximately 56.7 kg (125 lb). Three persons are required to safely move an empty tray. If the tray is populated with components, a mechanized lift is required to safely move the tray.

**WARNING!****Risk of bodily injury**

Each tray has more than one power cord. To remove all electrical current from the devices, make sure that all of the power cords are disconnected from the power source and that the two-pole 20-amp circuit breaker for the storage array has been disconnected.

**WARNING!****Risk of bodily injury**

Each tray has more than one power cord. To remove all electrical current from the devices, make sure that all of the power cords are disconnected from the power source.

**WARNING!****Risk of bodily injury**

Do not use equipment in the cabinet as a shelf or work space.



1.2

Caution Notices

CAUTION!

Potentially hazardous material

The battery pack contains sealed lead acid batteries that might be considered hazardous material. If you recycle a used battery pack that is not damaged, use the proper facilities. Handle the battery pack according to all applicable regulations.

CAUTION!**Potentially hazardous material**

If the used battery pack is physically damaged or is leaking, DO NOT ship the battery pack to a recycling center. Handling a damaged battery pack exposes you and others to potentially hazardous material. Dispose of the damaged battery pack according to all applicable regulations.

CAUTION!**Pinching hazard**

As you push the canister into the slot, ensure that your fingers are not pinched between the lever and the canister. The lever automatically moves toward the closed position as the canister is pushed into its slot.

CAUTION!**Potentially hazardous material**

The battery pack contains sealed lithium ion batteries that might be considered hazardous material. If the used battery pack is physically damaged and is leaking, DO NOT ship the battery pack to a recycling center. Handling a damaged battery pack exposes you and others to potentially hazardous material. Dispose of the damaged battery pack according to all applicable regulations. If you recycle a used battery pack that is not damaged, use the proper facilities. Handle the battery pack according to all applicable regulations.

CAUTION!**Electrical grounding hazard**

This equipment is designed to permit the connection of the DC supply circuit to the earthing conductor at the equipment.

CAUTION!**Possible hazard exists**

Do not remove more than one canister from the enclosure while power to the enclosure is turned on.

2

General

This document describes the tasks necessary for installing and starting SANtricity ES Storage Manager for Version 10.80, and then performing initial configuration on your storage array. Consult this topic after configuring and cabling the storage array through one of the hardware configuration guides for the E2600 controller-drive tray.

3 Deciding on the Management Method

You can manage a storage array using the in-band method, the out-of-band method, or both.

Note:

You need to know the storage management method that you plan to use before you install the SANtricity ES Storage Manager software and use the storage management software.

3.1 Key Terms

access volume

A special volume that is used by the host-agent software to communicate management requests and event information between the management station and the storage array. An access volume is required only for in-band management.

Dynamic Host Configuration Protocol (DHCP)

CONTEXT [Network] An Internet protocol that allows nodes to dynamically acquire ('lease') network addresses for periods of time rather than having to pre-configure them. DHCP greatly simplifies the administration of large networks, and networks in which nodes frequently join and depart. (The Dictionary of Storage Networking Terminology)

in-band management

A method to manage a storage array in which a storage management station sends commands to the storage array through the host input/output (I/O) connection to the controller.

out-of-band management

A method to manage a storage array in which a storage management station sends commands to the storage array through the Ethernet connections on the controller.

stateless address autoconfiguration

A method for setting the Internet Protocol (IP) address of an Ethernet port automatically. This method is applicable only for IPv6 networks.

World Wide Identifier (WWID)

CONTEXT [Fibre Channel] A unique 64-bit number assigned by a recognized naming authority (often using a block assignment to a manufacturer) that identifies a node process or node port. A WWID is assigned for the life of a connection (device). Most networking physical transport network technologies use a world wide unique identifier convention. For example, the Ethernet Media Access Control Identifier is often referred to as the MAC address. The Dictionary of Storage Networking Terminology)

3.2 Procedure – Management Method

Note:

If you use the out-of-band management method but do not have a DHCP server, you must manually configure your controllers. See *Section 12 Manually Configuring the Controllers, page 51* for details.

1. Use the key terms and the following figures to determine the management method that you will use.

- 2. After reading the information in this section, add a check mark next to the management method that you will use.
 - In-band management method
 - Out-of-band management method
 - In-band management method and out-of-band management method

Note:

A host system with a host bus adapter (HBA) can run the storage management software; you do not need to install the management client on a separate client system

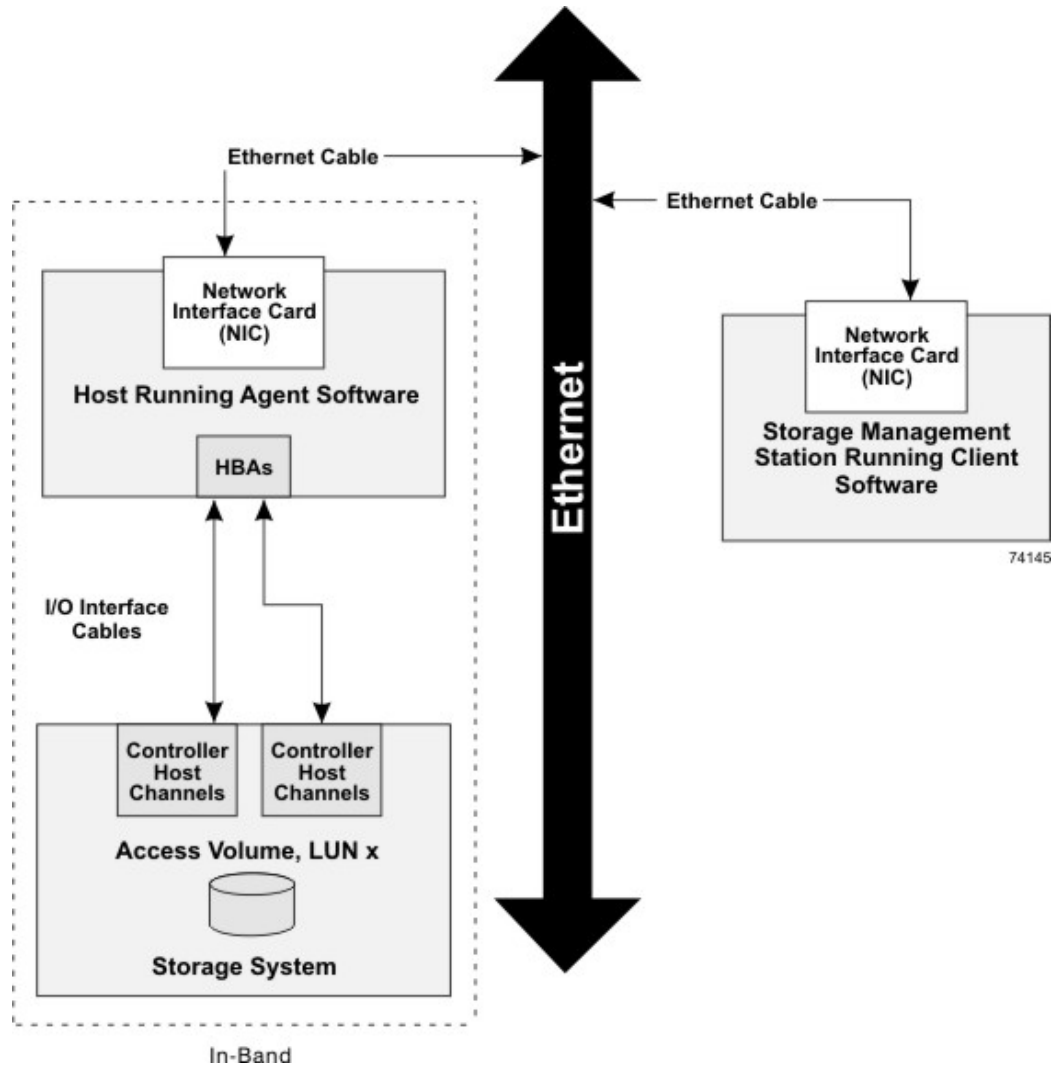


Figure 3.1 In-Band Management Topology

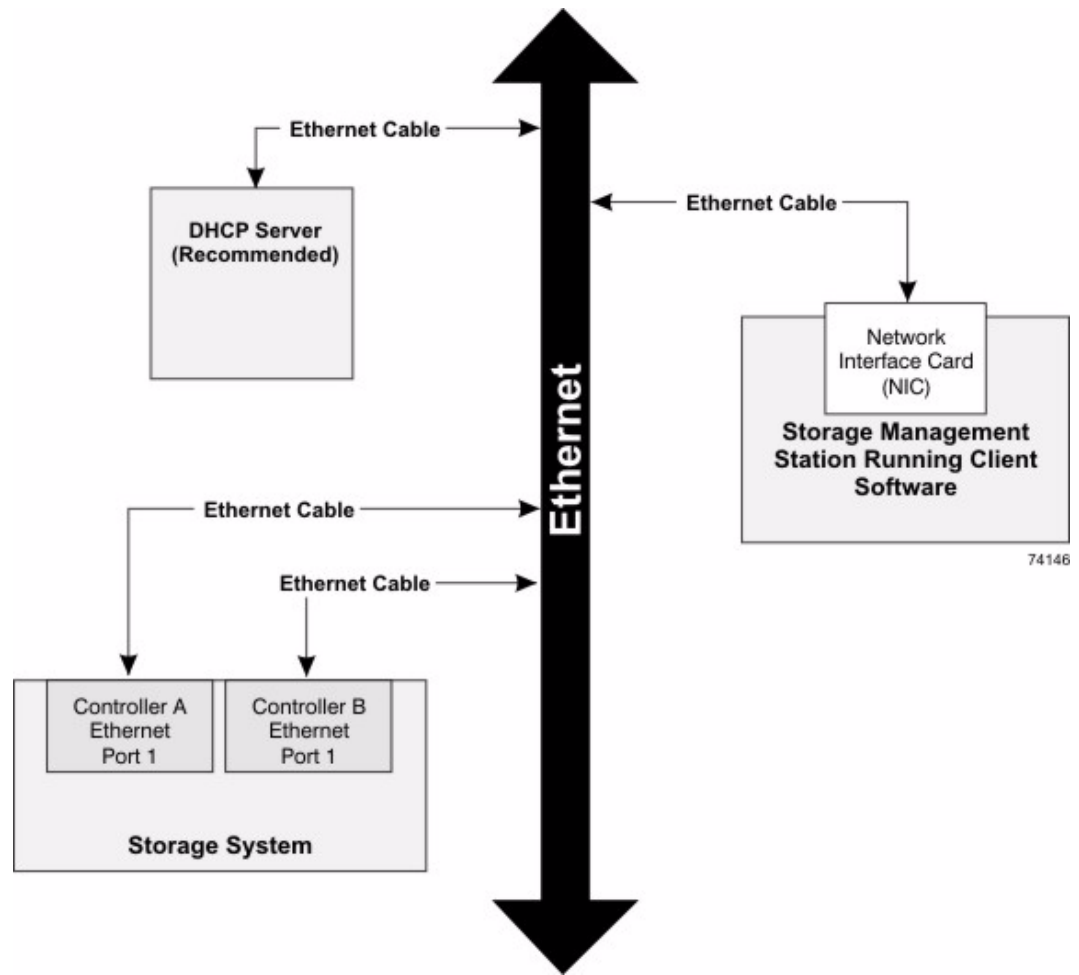


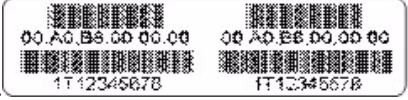
Figure 3.2 Out-of-Band Management Topology

3.3 Things to Know – In-Band and Out-of-Band Requirements

Table 3.1 Out-of-Band and In-Band Management Requirements

Management Method	Requirements	Advantages	Disadvantages
Out-of-band without a DHCP server	Connect separate Ethernet cables to each controller. Manually configure the network settings on the controllers. See <i>Section 12 Manually Configuring the Controllers, page 51</i> for more information.	This method does not use a logical unit number (LUN) on the host. You do not need to install the host-agent software. This method does not use the SAS, Fibre Channel, or iSCSI bandwidth for storage array management functions.	You must manually configure the network settings on the controllers. Ethernet cables are required.
Out-of-band – IPv6 stateless address auto-configuration without a DHCP server (IPv6 networks only)	Connect separate Ethernet cables to each controller. Connect at least one router for sending the IPv6 network address prefix in the form of router advertisements.	No additional manual network configuration is required on the controllers. By default, the controllers automatically obtain their IP addresses by combining the auto-generated link local address and the IPv6 network address prefix after you turn on the power to the controller-drive tray. You do not need to install host-agent software. This method does not use a LUN on the host. This method does not use the Fibre Channel or iSCSI bandwidth for storage array management functions.	Ethernet cables are required.

Table 3.1 Out-of-Band and In-Band Management Requirements

Management Method	Requirements	Advantages	Disadvantages
Out-of-band with a DHCP server (IPv4 networks only)	<p>Connect separate Ethernet cables to each controller. Assign either static IP addresses or dynamic IP addresses to the controllers. It is recommended that you assign static IP addresses. Check your DHCP server for the IP addresses that are associated with the media access control (MAC) addresses of the controllers. The MAC address appears on a label on each controller in the form:</p> <p>xx.xx.xx.xx.xx.xx</p> 	<p>No additional manual network configuration is required on the controllers. By default, the controllers automatically obtain their IP addresses from the DHCP server after you turn on the power to the controller-drive tray. You do not need to install host-agent software. This method does not use a LUN on the host. This method does not use the Fibre Channel or iSCSI bandwidth for storage array management functions.</p>	Ethernet cables are required.
In-band	<p>Install host-agent software on at least one of the network-attached hosts. The host-agent software is included with the storage management software. This method requires a special access volume to communicate. This volume is created automatically.</p>	No additional manual network configuration is required on the controller.	This method uses both a LUN on the host and the Fibre Channel bandwidth for storage array management functions.

4 Setting Up the Storage Array for Windows Server 2008 Server Core

If your host is running Windows Server 2008 Server Core, use the procedures in this section to configure your storage array. Before you perform the procedures in this section, make sure that you have completed the relevant hardware configuration.

- If your host is not running Windows Server 2008 Core, go to *Section 5 Installing the SANtricity ES Storage Manager Software, page 22* to continue the installation.
- If your host is running Windows Server 2008 Server Core, you must use the command line and the procedures in this topic to install and configure your storage array.

If you are using iSCSI host connections, perform the procedures in this section to configure the iSCSI initiator and to install the storage management software:

1. Configure the network interfaces.
2. Set the iSCSI initiator services.
3. Install the storage management software (in lieu of completing the task from *Section 5 Installing the SANtricity ES Storage Manager Software, page 22*).
4. Configure the iSCSI ports.
5. Configure and view the targets.
6. Establish a persistent login to a target.
7. Verify your iSCSI configuration.
8. Review other useful iSCSI commands.
9. Configure your storage array.

Refer to the *Microsoft iSCSI Software Initiator 2.x Users Guide* for more information about the commands used in these steps.

Refer to the *Microsoft Developers Network (MSDN)* for more information about Windows Server 2008 Server Core.

You can access these resources from www.microsoft.com.

If you are using either Fibre Channel or SAS host connections, you must also perform these additional procedures:

1. Install the storage management software using *Section 5 Installing the SANtricity ES Storage Manager Software, page 22*.
2. Configure your storage array using *Section 19 Configuring the Storage, page 66*.

4.1 Procedure – Configuring the Network Interfaces

1. Find the index for the iSCSI initiator by typing one of these commands and pressing

Enter:

- C:\>netsh interface ipv4 show interfaces
- C:\>netsh interface ipv6 show interfaces

A list of all found interfaces appears (see table below):

2. Set the IP address for the initiators.

For IPv4 initiators, type these commands from the command line:

- C:\Users\administrator>netsh interface ipv4 set address name=3 source=static address=192.168.0.1 mask=255.255.255.0
- C:\Users\administrator>netsh interface ipv4 set address name=4 source=static address=192.168.1.1 mask=255.255.255.0

For IPv6 initiators, type these commands from the command line:

- C:\Users\administrator>netsh interface ipv6 set address name=3 source=static address=<IPv6 address> mask=255.255.255.0
- C:\Users\administrator>netsh interface ipv6 set address name=4 source=static address=<IPv6 address> mask=255.255.255.0

In the previous two commands, <IPv6 address> is the IPv6 address for the iSCSI initiator.

Table 4.1 Found Interfaces

Idx	Met	MTU	State	Name
2	10	1500	connected	Local Area Connection
1	50	4294967295	connected	Loopback Pseudo-Interface 1
3	20	1500	connected	Local Area Connection 2
4	20	1500	connected	Local Area Connection 3

4.2

Procedure – Setting the iSCSI Initiator Services

Set the iSCSI initiator services to start automatically. From the command line, type this command:

```
sc\server_name config msiscsi start=auto
```

In this command, `server_name` is the name of the host.

4.3

Procedure – Installing the Storage Management Software

The SANtricity ES Storage Manager executable is located on the SANtricity ES Storage Manager Installation DVD.

1. Insert the DVD into the host DVD drive.
2. Locate the installation package that you want to install. From the command line, type one of these commands:

```
<hsw executable.exe> -i console
```

```
<hsw executable.exe> -i silent
```

In these commands, <hsw executable.exe> is the file name for the storage management software installation package.

When you specify the `console` parameter during the installation, questions appear on the console that enable you to choose installation variables. This installation does not use a graphical user interface (GUI). Contact your Customer and Technical Support representative if you need to change the installation options.

When you specify the `silent` parameter during the installation, the command installs the storage management software using all of the defaults. A silent installation uses a resource file that contains all of the required information, and it does not return any windows until the installation is complete. This installation does not use a graphical user interface (GUI). Contact your Customer and Technical Support representative if you need to change the installation options.

3. Make sure that the appropriate files are listed in the installation directory. A full installation should include these directories:
 - util (SMutil)
 - client (SMclient)
 - agent (SMagent)
4. Type this SMcli command without options to make sure that SMcli was installed correctly.

```
SMcli <controller_A_IP_address> <controller_B_IP_address>
```

Note:
In the Windows operating system, you must perform this command from the `client` directory.
5. Make sure that an **Incorrect Usage** message is returned with a list of allowable SMcli options.

Note:
To make sure that your configuration settings take effect, you must reboot the host before starting the storage management software.

4.4 Procedure – Configuring the iSCSI Ports

Use the command line interface that is included in the storage management software to configure the iSCSI ports. Refer to the *Command Line Interface and Script Commands for Version 10.77* electronic document topics for instructions on how to configure the iSCSI ports. The information in the programming guide applies to the SANtricity ES Storage Manager software. You must complete these tasks:

1. Show a list of unconfigured iSCSI initiators.
2. Create an iSCSI initiator.
3. Set the iSCSI initiator.
4. Set the iSCSI target properties.
5. Show the current iSCSI sessions.

4.5 Procedure – Configuring and Viewing the Targets

Configure a target and, optionally, persist that target. You must configure each port on the target one time. If you are using Challenge-Handshake Authentication Protocol (CHAP), you can also establish a CHAP user name and password when you configure the target.

1. Are you using CHAP?
 - If yes, go to step 3.
 - If no, go to step 2.
2. If you are not using CHAP, type this command for each port on the target from the command line. When you are finished, go to step 4.

```
iscsicli QAddTargetPortal <IP Address Target Controller>
```

In this command, `<IP Address Target Controller>` is the IP address for the target port that you are configuring.

3. If you are using CHAP, type this command for each port on the target from the command line. When you are finished, go to step 4.

```
iscsicli QAddTargetPortal <IP Address Target Controller> <CHAP
Username> <CHAP Password>
```

In this command:

- <IP Address Target Controller> is the IP address for the target port that you are configuring.
 - <CHAP Username> and <CHAP Password> are the optional user name and password for the target port that you are configuring.
4. After you have configured all of the ports on the target, you can show a list of all configured targets. From the command line, type this command:

```
iscsicli ListTargets
```

A list of all found targets appears.

4.6 Procedure – Establishing a Persistent Login to a Target

You can establish a persistent login to a target. A persistent login is the set of information required by an initiator to log in to the target each time the initiator device is started. The login usually occurs when you start the host. You cannot initiate a login to the target until after the host has finished rebooting. You must establish a persistent login for each initiator-target combination or initiator-target path. This command requires 18 parameters. Several of the parameters use the default values and are indicated with *. Refer to the *Microsoft iSCSI Software Initiator 2.x Users Guide* for a description of this command and the parameters.

From the command line, type this command:

```
iscsicli PersistentLoginTarget <Target Name> <ReportToPNP>
<TargetPortalAddress> <TCPPortNumberofTargetPortal> * * * <Login Flags> * *
* * * * * * * <MappingCount>
```

In this command:

- <Target Name> is the name of your target port as shown in the targets list.
- <ReportToPNP> is set to T, which exposes the LUN to the operating system as a storage device.
- <TargetPortalAddress> is the IP address for the target port.
- <TCPPortNumberofTargetPortal> is set to 3260, which is the port number defined for use by iSCSI.
- <Login Flags> is set to 0x2, which allows more than one session to be logged into a target at one time.
- <MappingCount> is set to 0, which indicates that no mappings are specified and no further parameters are required.
- * uses the default value for that parameter.

Note:

To make sure that your configuration settings take effect, you must reboot the host before continuing with these tasks.

4.7 Procedure – Verifying Your iSCSI Configuration

After you reboot the host, you can verify your configuration.

From the command line, type this command:

```
iscsici ListPersistentTargets
```

A list of persistent targets configured for all iSCSI initiators appears. Make sure that “Multipath Enabled” appears in the output under Login Flags.

4.8 Procedure – Reviewing Other Useful iSCSI Commands

The commands listed in this section are useful for managing the iSCSI targets and iSCSI initiators.

This command shows the set of target mappings assigned to all of the LUNs to which all of the iSCSI initiators are logged in.

```
iscsicli ReportTargetMappings
```

This command shows a list of active sessions for all iSCSI initiators.

```
iscsicli sessionlist
```

This command sends a SCSI REPORT LUNS command to a target.

```
iscsicli ReportLUNS <SessionId>
```

This command removes a target from the list of persistent targets.

```
iscsicli RemovePersistentTarget <Initiator Name> <TargetName>  
<Initiator Port Number> <Target Portal Address> <Target Portal Socket>
```

These commands and others are described in the Microsoft iSCSI Software Initiator 2.x Users Guide.

4.9 Procedure – Configuring Your Storage Array

You have these methods for configuring your storage array:

- You can configure the storage array from a storage management station that is on the same network as the storage array. This method is preferred. Continue to Go to *Section 6 Configuring the Host Bus Adapters, page 30*, and then make sure that you complete the *Section 19 Configuring the Storage, page 66* to finish configuring your storage array.
- You also can configure the storage array using the command line interface. Refer to *Secton Configuring a Storage Array* in the *Configuring and Maintaining a Storage Array Using the Command Line* electronic document topic for information that will help you configure your storage array.

5 Installing the SANtricity ES Storage Manager Software

If you are running Windows Server 2008 Server Core, make sure that you have performed the tasks in *Section 4 Setting Up the Storage Array for Windows Server 2008 Server Core, page 17*. If you are not running Windows Server 2008u Server Core, start with the tasks in this step.

5.1 Key Terms

host

A computer that is attached to a storage array. A host accesses volumes assigned to it on the storage array. The access is through the HBA host ports or through the iSCSI host ports on the storage array.

monitor

A software package that monitors the storage array and reports critical events.

multi-path driver

A driver that manages the input/output (I/O) data connection for storage arrays with redundant controllers. If a component (cable, controller, host adapter, and so on) fails along with the I/O data connection, the multi-path driver automatically reroutes all I/O operations to the other controller.

Redundant Dual Active Controller (RDAC) multi-path driver

A driver that manages the I/O data connection for storage arrays with dual controllers in a redundant configuration. If a component fails along the connections, causing the host to lose communication with a controller, the driver automatically reroutes all I/O operations to the other controller.

storage management station

A computer running storage management software that adds, monitors, and manages the storage arrays on a network.

5.2 Things to Know – All Operating Systems

This section describes how to use the installation wizard to install the SANtricity ES Storage Manager software (hereinafter referred to as the storage management software). The separate native installation packages are supplied on the SANtricity ES Storage Manager Installation DVD in the `native` directory.

For the Windows Server 2003 operating system (OS), the Windows Server 2008 OS, the Linux OS, the Solaris OS, and VMware, the storage management software supports using the storage array as a boot device. For assistance with setting up this configuration, contact your Customer and Technical Support representative.

**NOTICE!**

If the Windows Server 2003 OS, the Windows Server 2008 OS, or the Linux OS is installed on a computer with an Intel Itanium 2 (IA64) processor, you cannot use the storage array as a boot device.

5.3 Things to Know – Specific Operating Systems

Solaris OS:

- The Solaris OS supports the use of the Multiplexed I/O (MPxIO) driver.
- The Solaris OS supports the use of the Sun Cluster software for clustering.

Windows XP OS and Windows Vista OS:

- These operating systems support the SANtricity ES Storage Manager Client package only.
- Other storage management software packages are not available on the Window XP OS and the Windows Vista OS, including the failover driver.
- Systems running these operating systems can be used only as storage management stations.
- Providers for Microsoft Virtual Disk Service (DVDS), Microsoft Volume Shadow Copy Service (VSS), and Storage Networking Industry Association (SNIA) are not supported on these operating systems.

Windows Server 2003 OS SP2 R2 and Windows Server 2008 OS R2 SP1:

- When the RDAC multi-path driver is not installed, the **Install Complete** window shows an error message that states that the installation is finished and that some warnings exist. The message suggests looking at the installation log for details. The installation log contains a warning that a Win32 exception can be found. This behavior is normal and expected. The installation was successful.
- These operating systems support the use of the Microsoft Multi-Path I/O (MPIO) driver for failover.

Linux Red Hat 5.6 Client OS, Linux Red Hat 6 Client OS, SUSE Desktop 10 OS, and SUSE Desktop 11.1 OS:

- These operating systems support only the SANtricity ES Storage Manager Client package.
- Other storage management software packages are not available on the Linux Red Hat 5 Client OS and the SUSE Desktop 11.1 OS, including the failover driver.
- Systems running these operating systems can be used only as storage management stations.

Red Hat Enterprise Linux OS and SUSE Linux Enterprise Server OS:

- These operating systems support the use of the LSI RDAC multi-path driver for failover.
- Both the Linux Red Hat 6 Client OS and the SUSE Desktop 11.1 OS also support the native device mapper application.
- These operating systems support the use of the SteelEye® LifeKeeper and Native Red Hat Clustering software for clustering.

5.4 Things to Know – System Requirements

The following tables describe the operating system specifications, memory requirements, and disk space requirements.

Table 5.1 Operating System Version or Edition Requirements

Operating System	System and Version or Edition
Windows XP	x86-based system (32-bit and 64-bit)Pentium or greater CPU or equivalent (233 MHz minimum)Professional Service Pack 3 (SP3) or later NOTE – Storage management station only.
Windows Server 2003 SP2 R2	Standard Server Edition system (32-bit and 64-bit)Enterprise Edition, (32-bit and 64-bit)Datacenter Edition, (32-bit and 64-bit)x64 Edition (AMD and EM64T support)x86-based system (AMD64 and EM64T)Web Edition (client only version with no failover support)
Windows Vista	SP1 x86-based system (32-bit and 64-bit)Pentium or greater CPU or equivalent (800 MHz minimum) NOTE – Storage management station only.

Table 5.1 Operating System Version or Edition Requirements

Operating System	System and Version or Edition
Windows Server 2008 R2 SP1	x86-based system (64-bit only: AMD64 and EM64T)Standard Server and Core EditionEnterprise Server and Core EditionDatacenter Server and Core EditionFoundation Server and Core EditionWeb Edition (client only version with no failover support)
Windows Hyper-V Server 2008 R2 SP1(standalone)	x86-based system (64-bit only: AMD64 and EM64T)
VMware	3.5u5+P204.1AMD64 and EM64T Note: The VMware 3.5 OS does not support configurations with any versions of the CE5400 controller-drive tray.
Macintosh OS X	10.5.810.6.3Intel Xeon x86 64-bit support only
Linux	Intel Xeon EM64T and AMD Opteron 32-bit and 64-bit processorsRed Hat Enterprise Linux 5.5Red Hat Enterprise Linux 6.0SUSE Linux Enterprise Server 10 SP 3SUSE Linux Enterprise Server 11 SP1Client only versions (all 32-bit only with no I/O attach): <ul style="list-style-type: none"> – Red Hat Enterprise Linux 5.0 client – Red Hat Enterprise Linux 6.0 client – SUSE Linux Enterprise Server 10 client – SUSE Linux Enterprise Server 11 client
Linux (Infiniband)	Red Hat Enterprise Linux 6.0 (Mellanox driver)SUSE Linux Enterprise Server 11 SP1 (Mellanox driver)Support only for 64-bit versions of the operating systems (EM64T and AMDx86)Client only versions: <ul style="list-style-type: none"> – Red Hat Enterprise Linux 5.0 client – Red Hat Enterprise Linux 6.0 client – SUSE Linux Enterprise Server 10 client – SUSE Linux Enterprise Server 11 client
HP-UX	11.31 March 2010 (IA64 and PA-RISC)Fibre Channel only (direct connection)
Solaris	SPARC-based systemx86-based system (Intel Xeon, and 32-bit AMD Opteron or 64-bit AMD Opteron)Solaris 10 Update 9

Table 5.2 Temporary Disk Space Requirements

Operating System	Available Temporary Disk Space	Other Requirements
Windows XP	255 MB	–
Windows Server 2003	291 MB	–
Windows Vista	291 MB	–
Windows Server 2008	291 MB	–
Linux	390 MB	–
HP-UX	582 MB	–
Solaris	540 MB	–

Note:

The minimum RAM requirement is 512 MB.

5.5 Procedure – Installing the SANtricity ES Storage Manager Software

Note:

Make sure that you have the correct administrator or superuser privileges to install the software.

1. Insert the SANtricity ES Storage Manager Installation DVD in the DVD drive.
Depending on your operating system, a program autoplays and shows a menu with installation selections. If the menu does not appear, you must perform these tasks:
 - Manually open the `install` folder.
 - Locate the installation package that you want to install.
2. Install the software installation packages that are required for your storage configuration. You might be required to open a window or terminal to run one of these commands.

- `hsw_executable.exe -i console`
- `hsw_executable.exe -i silent`

In the commands, `hsw_executable.exe` is the file name for the storage management software installation package.

- When using the `console` parameter during the installation, questions appear on the console that enable you to choose installation variables. This installation does not use a graphical user interface (GUI). Contact your Customer and Technical Support representative if you need to change the installation options.
- When using the `silent` parameter during the installation, the command installs the storage management software using all of the defaults. A silent installation uses a resource file that contains all of the required information, and it does not return any windows until the installation is complete. This installation does not use a GUI. Contact your Customer and Technical Support representative if you need to change the installation options.

Example:

These examples show the actual command used to launch the installation wizard for a particular operating system.

- **Windows operating systems** – Double-click the executable file. In general, the executable file begins with SMIA followed by the operating system name, such as `SMIA-WS32.exe`.
- **UNIX operating systems** – At the command prompt, type the applicable command to start the installer, and press Enter. For example, type a command that is similar to this command: `sh DVD_name.bin`. In this command, `DVD_name.bin` is the name of the installation DVD, such as `SMIA-LINUX.bin`.

If necessary, set the display environment to issue the command.

Example: Use the information in the on-screen instructions to install the software.

5.6 Things to Know – Software Packages

Client – This package contains the graphical user interface for managing the storage array. This package also contains a monitor service that sends alerts when a critical problem exists with the storage array.

**NOTICE!**

You can add from one to eight clients to your storage configuration.

Utilities – This package contains utilities that let the operating system recognize the volumes that you create on the storage array and to view the operating system-specific device names for each volume.

Agent – This package contains software that allows a management station to communicate with the controllers in the storage array over the I/O path of a host (see *Section 3.3 Things to Know – In-Band and Out-of-Band Requirements, page 15*).

Failover driver – This package contains the multi-path driver that manages the I/O paths into the controllers in the storage array. If a problem exists on the path or a failure occurs on one of the controllers, the driver automatically reroutes the request from the hosts to the other controller in the storage array.

Java Access Bridge (JAB) – This package contains accessibility software that enables Windows-based assistive technology to access and interact with the client application.

**NOTICE!**

The Microsoft Virtual Disk Service (VDS) and Volume Shadow Copy Service (VSS) providers are a part of the SANtricity ES Storage Manager package for the Windows Server 2003 OS and the Windows Server 2008 OS.

Use the figures and tables that follow to determine the software packages that should be installed on each machine. You must install the utilities and the failover driver on each host that is attached to the storage array.

**NOTICE!**

If you choose not to automatically enable the event monitor during installation, you will not receive critical alert notifications.

**NOTICE!**

During the client installation, you are asked whether you want to start the monitor. Start the monitor on only one host that runs continuously. If you start the monitor on more than one host, you receive duplicate alert notifications about problems with the storage array.

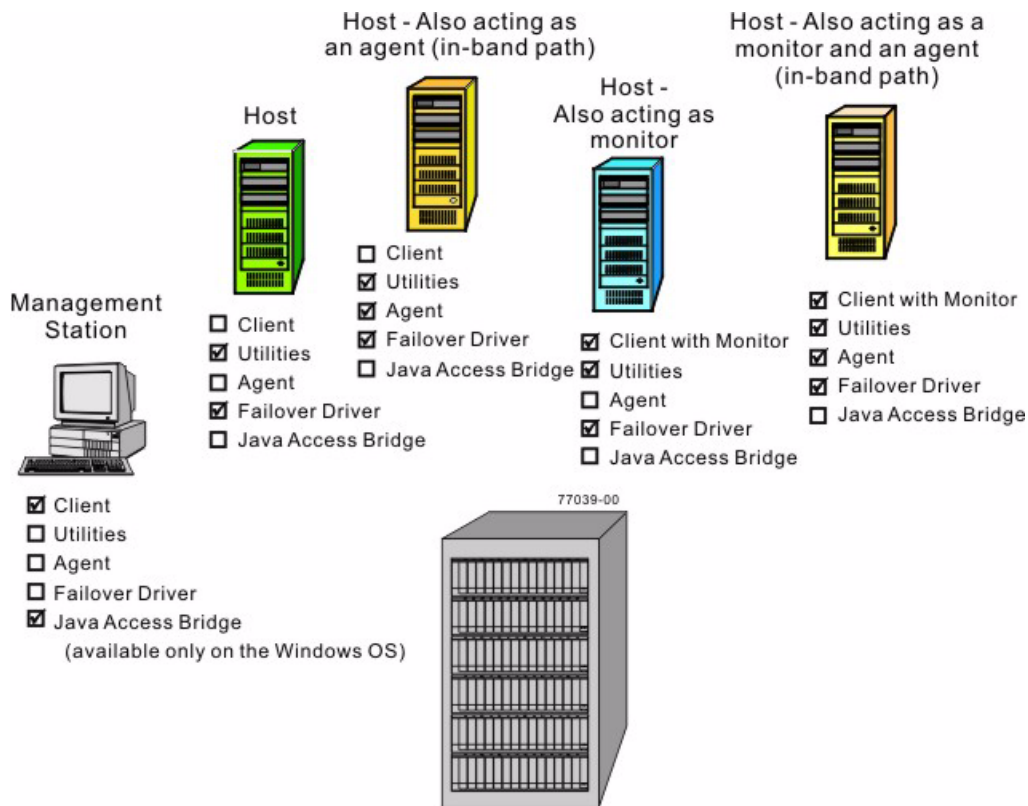


Figure 5.1 Software Configurations

Note:

The storage array is the box at the bottom of this figure.

Table 5.3 Different Machines and Required Software

Machine	Minimum Software Required	Installation Package (Choose One) (See the tables that follow)	Notes
Management station	Client	<ul style="list-style-type: none"> – Typical Installation – Management Station – Custom 	<ul style="list-style-type: none"> – Click No to the prompt, Automatically start Monitor? – You must choose Custom if you want to install the Java Access Bridge software.
Host	<ul style="list-style-type: none"> – Utilities – Failover driver 	<ul style="list-style-type: none"> – Typical Installation – Host – Custom 	<ul style="list-style-type: none"> – Click No to the prompt, Automatically start Monitor? – Be aware that some operating systems require the manual installation of the RDAC failover driver.

Table 5.3 Different Machines and Required Software

Machine	Minimum Software Required	Installation Package (Choose One) (See the tables that follow)	Notes
Host – Also acting as an agent for the in-band management method	<ul style="list-style-type: none"> – Utilities – Agent – Failover driver 	<ul style="list-style-type: none"> – Typical Installation – Host – Custom 	Click No to the prompt, Automatically start Monitor?
Host – Also acting as a monitor for sending critical alerts	<ul style="list-style-type: none"> – Client – Utilities – Failover driver 	<ul style="list-style-type: none"> – Typical Installation – Custom 	<ul style="list-style-type: none"> – Click Yes to the prompt, Automatically start Monitor? – Start the monitor on only one host that will run continuously.
Host – Also acting as an agent for the in-band management method and a monitor for sending critical alerts	<ul style="list-style-type: none"> – Client – Utilities – Agent – Failover driver 	<ul style="list-style-type: none"> – Typical Installation – Custom 	<ul style="list-style-type: none"> – Click Yes to the prompt, Automatically start Monitor? – Start the monitor on only one host that will run continuously.

Table 5.4 Installation Wizard Selections

Type of Installation	Client	Utilities	Agent	Failover	JAB
Typical Installation	X	X	X	X	–
Management Station	X	–	–	–	–
Host Station	–	X	X	X	–
Custom (you select the packages)	X	X	X	X	X
Note: Java Access Bridge – Enables Windows OS-based assistive technology to access and interact with the application.					

Table 5.5 Software Packages That Are Supported on Each Operating System

Operating System	Client	Utilities	Agent	Failover	JAB
Windows XP Professional SP3 and Windows Vista	X	–	–	–	X
Windows Server 2003 and Windows Server 2008	X	X	X	X	X
VMware 3.5 and 4.1	X	X ^a	X	X	–
Red Hat 5.0 Client and SUSE Linux Enterprise Desktop 10	X	–	–	X	–

Table 5.5 Software Packages That Are Supported on Each Operating System

Operating System	Client	Utilities	Agent	Failover	JAB
Red Hat 6.0 Client and SUSE Linux Enterprise Desktop 11.1	X	—	—	X	—
Red Hat Enterprise Linux and SUSE Linux Enterprise Server	X	X	X	Manual ^b	—
Solaris	X	X	X	X	—
Macintosh 10.5.8 and 10.6.3	—	X	X	X	X ^d
HP-UX 11.31 (FC only)	X ^c	X	X	X	—

^a If the Management client is run on a guest operating system, the only supported utility is SMdevices on an iSCSI HBA when the storage is directly attached to the guest operating system.

^b Refer to Failover Drivers and the *Making Sure that RDAC is Installed Correctly on the Linux OS*" topic

^c Both the Windows client and the Linux client are supported as well.

^d I/O attach only.

5.7 Procedure – Manually Installing RDAC on the Linux OS

- To change to the directory where the RDAC source was untarred, type this command, and press Enter:

```
cd linuxrdac
```

Note:
 For more information about installing RDAC, refer to the `Readme.txt` file in the `linuxrdac` directory.
- To clean the directory, type this command, and press Enter:

```
make clean
```
- To compile the trays, type this command, and press Enter:

```
make
```
- To install RDAC, type this command, and press Enter:

```
make install
```
- After the `make install` is completed, modify your bootloader configuration file. For more information about modifying the bootloader configuration, refer to the output from the `make install` command for Linux RDAC.
- Read the `Readme.txt` file in the `linuxrdac` directory to complete the RDAC installation process.
- Reboot or start your host.

6 Configuring the Host Bus Adapters

A host bus adapter (HBA) is an adapter on the information bus of the host computer. This adapter acts as a bridge and provides connectivity between both the host computer and the storage. Host bus adapters free up critical server processing time. Depending on the configuration of your storage array, you must set up the HBA to enable storage access using Fibre Channel (FC), iSCSI, SAS, or Infiniband connections. In addition, some operating system (OS) and failover driver settings may be necessary to make sure that your storage array runs properly.

6.1 Procedure – Configuring the HBAs

This section provides information about configuring your operating systems, failover drivers, and HBA settings for Fibre Channel (FC), iSCSI, and SAS protocols.

Use the following table to determine whether you need to make operating system, failover driver, or software initiator changes for your configuration. You will first need to make any operating systems changes, then alter failover driver settings, and finally make changes to the appropriate HBA, so work from left to right, using the appropriate settings for your particular configuration.



NOTICE!

No Change indicates that you do not need to modify the default settings, while 'Not applicable' indicates that the failover driver or software initiator does not apply to that particular operating system.

Table 6.1 Configuration Changes for Operating Systems, Failover Drivers, and HBAs

Operating Systems	Failover Drivers	FC Host Adapter	SAS Host Adapter Protocol	iSCSI Host Adapter or Software Initiator Protocol
Linux with MPP Failover Drivers		– – –		
Linux with DMMP Failover Drivers		– – –		
Windows		– – –		
VMware with ESX 3.5 or ESX 4.1	No change is required to any of the failover driver settings.	No change is required to any of the Emulex FC HBA settings.		No change is required to the iSCSI HBA with ESX 3.5.

Table 6.1 Configuration Changes for Operating Systems, Failover Drivers, and HBAs

Operating Systems	Failover Drivers	FC Host Adapter	SAS Host Adapter Protocol	iSCSI Host Adapter or Software Initiator Protocol
HP-UX	Not applicable	No changes are required to the HP-UX FC HBA settings.	Not applicable	Not applicable
Sun Solaris	Sun Solaris systems use the MPXIO failover driver, which requires no changes.	No changes are required to either the QLogic or the Emulex HBA settings.	Not applicable	Not applicable

6.2 Things to Know – Changing to Linux Operating System Settings, Failover Driver Settings, and HBA Settings for DMMP

Use the following table to determine the changes required by the Linux operating systems to either failover drivers or HBA settings when using the DMMP failover driver.

Table 6.2 Linux OS DMMP Failover Driver Configuration Changes

Linux OS DMMP Failover Driver Configuration Changes
Setting name: <code>dev_loss_tmo</code> Default value: 10 Recommended value: 15 Setting location: <code>/etc/multipath.conf</code> Comments: Driver time-out value.
Setting name: <code>failback</code> Default value: manual failback Recommended value: 10 Setting location: <code>/etc/multipath.conf</code> Comments: This change applies to non-cluster configurations only. For cluster configurations, do not change this value from the default.
Setting name: <code>fast_io_fail_tmo</code> Default value: 5 Recommended value: 10 Setting location: <code>/etc/multipath.conf</code> Comments: The midlayer uses either this value or the <code>dev_loss_tmo</code> , whichever is set to a lower value. If fast failover is set, some errors normally retried by the driver are immediately transferred to the alternate path.
Setting name: <code>features</code> Recommended value: <code>2 pg_init_retries 50</code> Setting location: <code>/etc/multipath.conf</code> Comments: This parameter allows for a higher number of mode-select retries, because the SLES 11.0 OS transfers only one LUN at a time.
Setting name: <code>getuid_callout</code> Default value: <code>"/lib/udev/scsi_id -- whitelisted -- device=/dev/%n"</code> Recommended value: <code>"/lib/udev/scsi_id -g -u -d/dev/%n"</code> Setting location: <code>/etc/multipath.conf</code>

Table 6.2 Linux OS DMMP Failover Driver Configuration Changes

Linux OS DMMP Failover Driver Configuration Changes
Setting name: <code>hardware_handler</code> Recommended value: <code>1 rdac</code> Setting location: <code>/etc/multipath.conf</code> Comments: This parameter sets the rdac device handler.
Setting name: <code>no_path_retry</code> Default value: <code>0</code> Recommended value: <code>30</code> Setting location: <code>/etc/multipath.conf</code> Comments: This midlayer uses either this setting or the <code>dev_loss_tmo</code> (whichever value is lower). If a fast failover is set, some errors that are normally retried by the driver are transferred to the alternate path.
Setting name: <code>path_checker</code> Default value: <code>directio</code> Recommended value: <code>rdac</code> Setting location: <code>/etc/multipath.conf</code>
Setting name: <code>path_grouping_policy</code> Default value: <code>multibus</code> Recommended value: <code>group_by_prio</code> Setting location: <code>/etc/multipath.conf</code>
Setting name: <code>path_selector</code> Default value: <code>round-robin 0</code> Recommended value: <code>round-robin 0</code> Setting location: <code>/etc/multipath.conf</code>
Setting name: <code>polling_interval</code> Default value: <code>5</code> Recommended value: <code>5</code> Setting location: <code>/etc/multipath.conf</code>
Setting name: <code>prio</code> Recommended value: <code>rdacS</code> Setting location: <code>/etc/multipath.conf</code>
Setting name: <code>rr_min_io</code> Default value: <code>1000</code> Recommended value: <code>100</code> Setting location: <code>/etc/multipath.conf</code>
Setting name: <code>rr_weight</code> Default value: <code>uniform</code> Recommended value: <code>priorities</code> Setting location: <code>/etc/multipath.conf</code>

Table 6.3 Linux OS FC Brocade HBA Changes for DMMP Failover Driver

Setting Changes
Setting name: <code>path_tov</code> Default value: <code>0x1E</code> Recommended value: <code>0xA</code>

Table 6.4 Linux OS FC Emulex HBA Changes for DMMP Failover Driver

Setting Changes
Setting name: <code>lpfc_devloss_tmo</code> Recommended value: 10 Setting location: <ul style="list-style-type: none"> - For the SLES11.0 OS and all subsequent releases: <code>/etc/modprobe.conf.local</code> - For the RHEL6 OS: <code>/etc/modprobe.d/</code> with <code>"options lpfc_devloss_tmo=10"</code>

Table 6.5 Linux OS FC QLogic HBA Changes for DMMP Failover Driver

Setting Changes
Setting name: <code>qlport_down_retry</code> Recommended value: 10 Setting location: <ul style="list-style-type: none"> - For SLES11.0 and all subsequent releases: <code>/etc/modprobe.conf.local</code> - For RHEL6: <code>/etc/modprobe.d/</code> with <code>"options qla2xxx qlport_down_retry=10"</code>

Table 6.6 Linux OS iSCSI HBA Changes for DMMP Failover Driver

Setting Changes
Setting name: <code>node.session.timeo.replacement_timeout</code> Default value: 120 Recommended value: 20 Setting location: <code>/etc/iscsi/iscsid.conf</code>
Setting name: <code>node.startup</code> Recommended value: <code>automatic</code> Setting location: <code>/etc/iscsi/iscsid.conf</code>
Setting name: <code>noop_out_interval</code> Recommended value: 5 Setting location: <code>/etc/iscsi/iscsid.conf</code>
Setting name: <code>noop_out_timeout</code> Recommended value: 5 Setting location: <code>/etc/iscsi/iscsid.conf</code>

6.3

Things to Know – Changing the Linux Failover Driver and HBA Settings for MPP

Use the following table to determine the changes required by the Linux MPP failover driver and the HBAs.

Table 6.7 MPP Failover Driver Configuration Changes

Setting Changes
Setting name: <code>DisableLunRebalance</code> Default value: <code>0x0</code> Recommended value: <code>0x3</code> Setting location: <code>/etc/mpp.conf</code> Comments: This setting applies only to cluster configurations.

Table 6.8 Linux OS FC Brocade HBA Changes for the MPP Failover Driver

Setting Changes
Setting name: <code>rport_del_timeout</code> Default value: <code>0x5a</code> Recommended value: <code>60</code> Setting location: <code>/etc/modeprobe.conf</code>

Table 6.9 Linux FC Emulex HBA Changes for MPP Failover Driver

Setting Changes
Setting name: <code>LinkTimeOut</code> Default value: <code>30</code> Recommended value: <code>60</code> Setting location: Use the Emulex HBAnyware application to change the location setting.
Setting name: <code>NodeTimeOut</code> Default value: <code>0x1E</code> Recommended value: <code>0X3c</code> Setting location: Use the Emulex HBAnyware application to change the location setting.

Table 6.10 Linux FC QLogic HBA Changes for MPP Failover Driver

Setting Changes
Setting name: <code>ExecutionThrottle</code> Default value: <code>0</code> Recommended value: <code>256</code> Setting location: Change this setting with both the QLogic BIOS for the in-the-box driver. Use the QLogic SANsurfer application for the standard driver.
Setting name: <code>qlport_down_retry</code> Default value: <code>30</code> Recommended value: <code>70</code> Setting location: <code>/etc/modprobe.conf</code> . Comments: Add " <code>options qlport_down_retry=70</code> " to the setting.

Table 6.11 Linux iSCSI Protocol Settings for the HBAs with the MPP Failover Driver

Setting Changes
Setting name: <code>node.session.timeo.replacement_timeout</code> Default value: <code>120</code> Recommended value: <code>144</code> Setting location: – For the SLES 11.0, the RHEL5 OS, and the RHEL6 OS: <code>/etc/iscsi/iscsid.conf</code> – For SLES 10.0: <code>/etc/iscsid.conf</code>
Setting name: <code>node.startup</code> Recommended value: <code>automatic</code> Setting location: – For the SLES 11.0 OS, the RHEL5 OS, and the RHEL6 OS: <code>/etc/iscsi/iscsid.conf</code> – For the SLES 10.0 OS: <code>/etc/iscsid.conf</code>

6.4 Things to Know – Changing Windows FC and iSCSI HBA Settings

Use the following tables to determine the changes required by the Windows OS to either failover drivers or HBA settings.

Table 6.12 Windows OS Configuration Changes for FC and iSCSI HBAs

Component	Setting Changes
Windows Server 2003 OS settings	Setting name: IO Timeout Value Default value: 0x14 Recommended value: 0x78 Recommended value when using iSCSI HBA: 0xA0 Setting location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\disk
Windows Server 2008 OS settings	Setting name: IO Timeout Value Default value: 0x14 Recommended value: 0x3c Setting location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\disk

Table 6.13 Windows Server 2003 OS and Windows Server 2008 OS MPIO/DSM Failover Driver Settings

Component	Setting Changes
MPIO/DSM failover driver settings for the Windows Server 2003 OS and the Windows Server 2008 OS	Setting name: DisableLunRebalance Default value: 0x0 Recommended value: 0x3 Setting location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mpcmds Comments: This setting only applies to MSCS cluster configurations.

Table 6.14 Brocade Fibre Channel HBA Settings for Windows

Component	Setting Changes
Brocade Fibre Channel HBA settings for the Windows Server 2008 OS	Setting name: path_tov Default value: 0x1E Recommended value: 0xA Comments: Use the Brocade BCU command line application to change the setting location.
Brocade Fibre Channel HBA settings for the Windows Server 2003 OS	Setting name: path_tov Default value: 0x1E Recommended value: 0x3C Comments: Use the Brocade BCU command line application to change the setting location.

Table 6.15 Emulex Fibre Channel HBA Settings for Windows

Component	Setting Changes
Emulex Fibre Channel HBA settings for the Windows Server 2008 OS	Setting name: <code>LinkTimeOut</code> Default value: <code>0x1E</code> Recommended value: <code>0xA</code> Comments: Use the Emulex HBAnywhere application to change the setting location.
	Setting name: <code>NodeTimeOut</code> Default value: <code>0x1E</code> Recommended value: <code>0xA</code> Comments: Use the Emulex HBAnywhere application to change the setting location.
Emulex Fibre Channel HBA settings for the Windows Server 2003 OS	Setting name: <code>LinkTimeOut</code> Default value: <code>30</code> Recommended value: <code>60</code>
	Setting name: <code>NodeTimeOut</code> Default value: <code>0x1E</code> Recommended value: <code>0x3C</code>

Table 6.16 Qlogic HBA Settings for Windows

Component	Setting Changes
Windows Server 2008 OS Fibre Channel Qlogic settings	Setting name: <code>ExecutionThrottle</code> Default value: <code>8</code> Recommended value: <code>255</code> Comments: Use the QLogic SANsurfer application to change the setting location.
	Setting name: <code>LinkDownTimeOut</code> Default value: <code>30</code> Recommended value: <code>10</code> Comments: Use the QLogic SANsurfer application to change the setting location.
	Setting name: <code>LunsPerTarget</code> Default value: <code>8</code> Recommended value: <code>0</code> Comments: Use the QLogic SANsurfer application to change the setting location.
	Setting name: <code>PortDownRetryCount</code> Default value: <code>30</code> Recommended value: <code>10</code> Comments: Use the QLogic SANsurfer application to change the setting location.

Table 6.16 Qlogic HBA Settings for Windows

Component	Setting Changes
Windows Server 2003 OS Fibre Channel Emulex settings	Setting name: ExecutionThrottle Default value: 8 Recommended value: 255 Comments: Use the Emulex HBAAnywhere application to change the setting location.
	Setting name: LinkDownTimeOut Default value: 30 Recommended value: 60 Comments: Use the Emulex HBAAnywhere application to change the setting location.
	Setting name: LoginRetryCount Default value: 8 Recommended value: 30 Comments: Use the Emulex HBAAnywhere application to change the setting location.
	Setting name: LunsPerTarget Default value: 8 Recommended value: 0 Comments: Use the Emulex HBAAnywhere application to change the setting location.
	Setting name: PortDownRetryCount Default value: 30 Recommended value: 70 Comments: Use the Emulex HBAAnywhere application to change the setting location.

Table 6.17 iSCSI HBA Settings for the Windows OS

Component	Setting Changes
Windows Server 2008 OS	Setting name: LinkDownTime Default value: 0x3C Recommended value: 0x1E Setting location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\XXX\parameters, where XXX is the only expandable folder.
Windows Server 2003 OS	Setting name: LinkDownTime Default value: 0x3C Recommended value: 0x90 Setting location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\XXX\parameters, where XXX is the only expandable folder.

6.5 Things to Know – Changing the SAS Host Adapters

Use the following table to see the changes required by the SAS HBA settings.

Table 6.18 SAS HBA Setting Changes

Component	Setting Changes
	For the Windows Server 2008 OS and the Linux OS using DMMP failover drivers, obtain the latest LSI SAS HBA firmware required settings from: http://kb.lsi.com/DownloadsCategory339.aspx .
	For the Windows Server 2003 OS and the Linux OS using MPP failover drivers, obtain the latest LSI SAS HBA firmware required settings from: http://kb.lsi.com/DownloadsCategory339.aspx . <ul style="list-style-type: none"> – Load the HBA firmware. – Change the settings that follow through the HBA BIOS.
SAS HBA settings for both the Windows 2003 OS and the Linux OSs with MPP failover drivers	Setting name: IODeviceMissingDelay Default value: 5 (the new default value with the customer firmware) Recommended value: 8 Comments: Use the HBA BIOS to change the setting location.
	Setting name: ReportDeviceMissingDelay Default value: 10 (the new default value with the customer firmware) Recommended value: 144 Comments: Use the HBA BIOS to change the setting location.

6.6

Things to Know – Changing the VMware OS HBA Settings

Use the following table to determine the changes required by the HBA settings when running on the VMware OS.

Table 6.19 QLogic FC HBA Settings on the VMware OS

Component	Setting Changes
QLogic FC host adapter changes	Setting name: qlink_down_timeout Default value: 30 Recommended value: 10 Comments: Change this setting through the QLogic SANsurfer application.
	Setting name: qlport_down_retry Default value: 15 Recommended value: 5 Comments: Change this setting through the QLogic SANsurfer application.

Table 6.20 SAS HBA Changes for the VMware OS

Component	Setting Changes
	You can obtain LSI SAS HBA firmware required settings from http://kb.lsi.com/DownloadsCategory339.aspx . Note: Make sure you load the HBA firmware first, then access the HBA BIOS to change the following settings.

Table 6.20 SAS HBA Changes for the VMware OS

Component	Setting Changes
SAS host adapter changes	Setting name: <code>IODeviceMissingDelay</code> Default value: 5 (new default with custom firmware) Recommended value: 0 Setting locations: You can alter the setting location in the HBA BIOS.
	Setting name: <code>ReportDeviceMissingDelay</code> Default value: 10 (new default with custom firmware) Recommended value: 0 Setting locations: You can alter the setting location in the HBA BIOS.

Table 6.21 iSCSI Host Adapter Changes for the VMware OS

Setting Changes
Setting name: <code>noop_out_interval</code> Default value: 40 Recommended value: 15 Setting locations: <code>vmkiscsi-tool -W -a "noop_out_interval=15" vmhba#</code> (where # is the iSCSI adapter number)
Setting name: <code>noop_out_timeout</code> Recommended value: 10 Setting locations: <code>vmkiscsi-tool -W -a "noop_out_timeout=10" vmhba#</code> (where # is the iSCSI adapter number)

6.7

Things to Know – Changing the HP-UX OS for HBAs

Make sure you make these changes after LUNs are visible to the OS.

Use the following table to determine the changes required by the HP-UX OS for the use of HBAs.

Table 6.22 HP-UX OS Changes for HBA

Setting Changes
Setting name: <code>Disk Timeout Value</code> Default value: 30 Recommended value: 120 Setting locations: <ul style="list-style-type: none"> - For the HP-UX 11iV2 OS and previous versions that use legacy device node – <code>#pvchange -t120/dev/dsk/c6t0d0</code> - For the HP-UX 11iV3 OS that uses the persistent DSF device node – <code>#pvchange -t120/dev/disk/disk_number</code>
Setting name: <code>IO Timeout Value</code> Recommended value: 240 Setting location: <code>#lvchange -t 240/dev/vg01/lvol1.</code>

7 Starting SANtricity ES Storage Manager

7.1 For Additional Information

For information about specific topics related to the SANtricity ES Storage Manager, refer to the following resources:

- *SANtricity ES Storage Manager Concepts for Version 10.80* electronic document topics.
- Online help topics in the Enterprise Management Window and the Array Management Window in SANtricity ES Storage Manager.

7.2 Procedure – Starting SANtricity ES Storage Manager

1. At the prompt, type `SMclient`, and press Enter.
2. Do the storage arrays appear in the Enterprise Management Window?
 - **Yes**
You are finished with this procedure.
 - **No**
A dialog asks whether to add the storage arrays automatically or manually. For the steps to add the storage arrays, see *Section 8 Adding the Storage Array, page 43*



NOTICE!

The Enterprise Management Window and the Array Management Window are the two main windows that you use to manage your storage array. The title at the top of each window identifies its type.

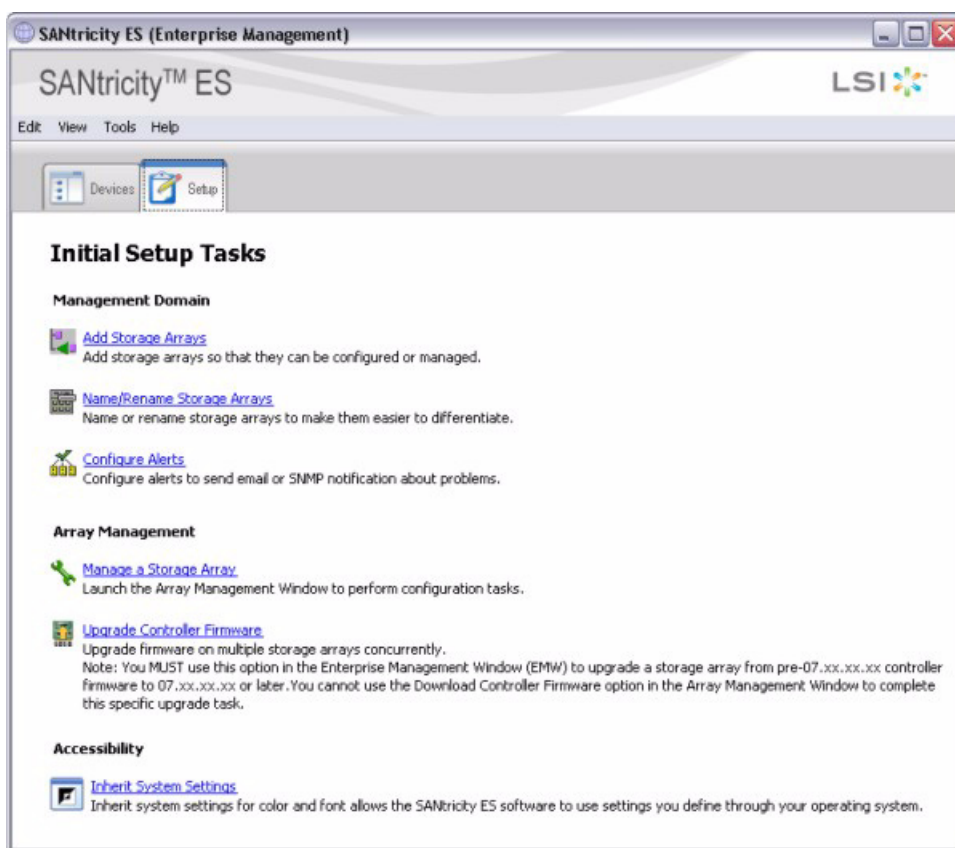
7.3 Things to Know – Enterprise Management Window and Array Management Window

Table 7.1 Overview of the Enterprise Management Window and the Array Management Window

User Interface	Description
Enterprise Management Window	<p>It is the main window that you see when you first start SANtricity ES Storage Manager.</p> <p>It provides you with a view of all of the storage arrays, including the partially managed storage arrays, in your management domain.</p> <p>It allows you to automatically or manually add and remove storage arrays, set alert notifications (email and SNMP), and perform other high-level configuration functions.</p> <p>It provides a high-level status of the health of each storage array.</p> <p>It allows you to manage and configure an individual storage array by launching the Array Management Window.</p>

Table 7.1 Overview of the Enterprise Management Window and the Array Management Window

User Interface	Description
Array Management Window	It provides you with all of the functions to configure, maintain, and troubleshoot an individual storage array. You launch the Array Management Window from the Enterprise Management Window to manage an individual storage array. Multiple Array Management Windows can appear at the same time (one for each storage array you want to manage).
Enterprise Management Window Setup Tab and Array Management Window Setup Tab	When you first start either the Enterprise Management Window or the Array Management Window, a Setup tab is selected by default. The Setup tab provides quick access to common setup tasks. The tasks shown are different, depending on the window from which the Setup tab was launched.



82005-01

Figure 7.1 Enterprise Management Window with the Setup Tab Selected

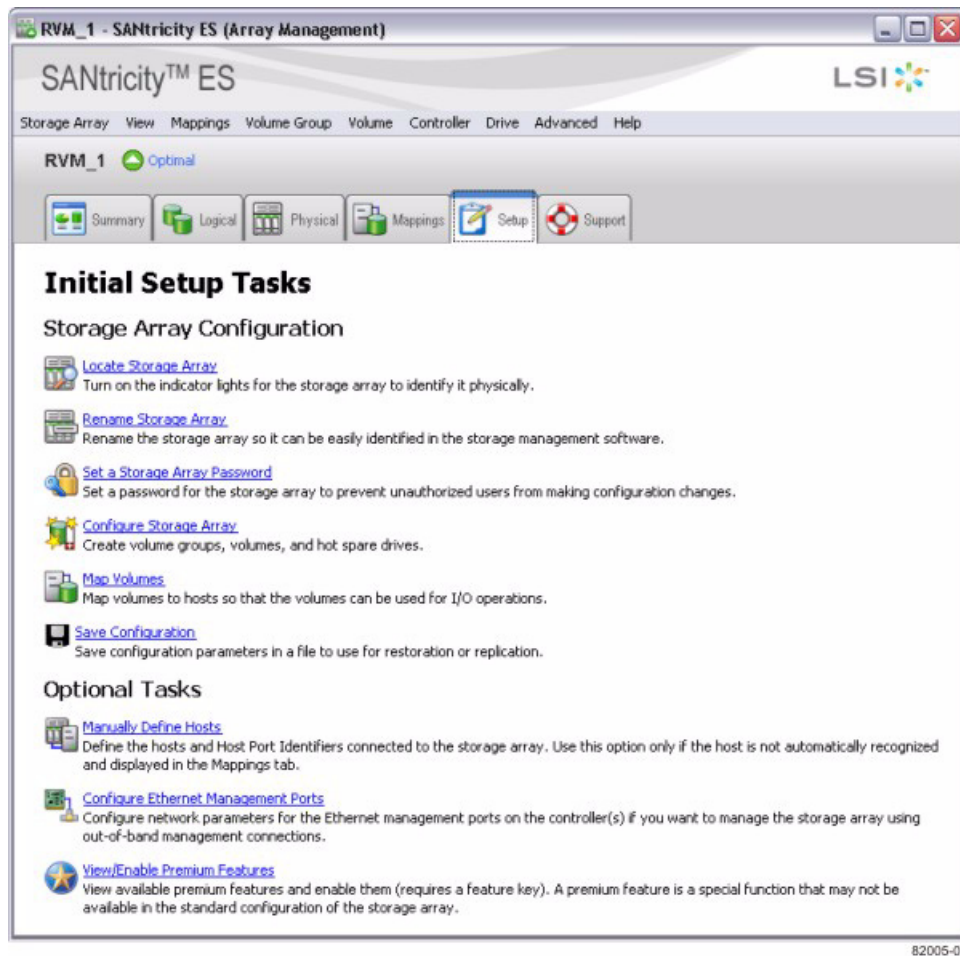


Figure 7.2 Array Management Window with the Setup Tab Selected

8 Adding the Storage Array

8.1 Things to Know – Storage Array

- Make sure that you have connected all of the applicable cables.
- Make sure that you have turned on the power to the storage array (attached drive trays first, and then the controller-drive tray or controller tray).
- Make sure that you have installed the applicable storage management software.

8.2 Procedure – Automatically Adding a Storage Array

1. From the Enterprise Management Window, select **Tools > Automatic Discovery**.
2. In the confirmation dialog, click **OK** to start the automatic discovery.
This process finds all of the storage arrays on the local sub-network. Several minutes might elapse to complete the process.
3. Do you see the storage array in the **Devices** tab of the Enterprise Management Window?
 - **Yes**
Go to *Section 9 Naming the Storage Array, page 46*.
 - **No** – Go to *Section 8.3 Procedure – Manually Adding a Storage Array, page 43* (the storage array might reside outside the local sub-network).



NOTICE!

After adding the storage array, you can view or change the cache memory settings of the storage array. See *Section 16 Changing the Cache Memory Settings, page 59*.

8.3 Procedure – Manually Adding a Storage Array

1. From the Enterprise Management Window, click the **Add Storage Arrays** link.
The **Add New Storage Array – Manual** dialog appears. By default, the **Out-of-band management** radio button is selected.

Figure 8.1 Add New Storage Array – Manual

2. Select one of the following radio buttons, depending on the type of management you are using:
 - Out-of-band – Select the **Out-of-band management** radio button.
 - In-band – Select the **In-band management** radio button.
3. Manually enter the host names or the IP addresses of the controllers (out-of-band management method) or the host name or IP address of the host that is running the host-agent software (in-band management method), and click **Add**.
The storage array appears in the Enterprise Management Window.



NOTICE!

You can enter the IP addresses in either the IPv4 format or the IPv6 format.



NOTICE!

After adding the storage array, you can view or change the cache memory settings of the storage array. See *Section 16 Changing the Cache Memory Settings, page 59*.

8.4 Things to Know – Rescanning the Host for a New Storage Array

You can rescan your host to perform these actions:

- Add new storage arrays that are connected to the host but are not shown in the Enterprise Management Window.
- Check the current status of storage arrays that are connected to the host.

**NOTICE!**

When you rescan your host for new storage arrays, you must stop and restart the host agent before selecting the rescan option.

8.5

Procedure – Rescanning the Host for a New Storage Array

1. From the **Devices** tab in the Enterprise Management Window, select the host that you want to rescan.

**NOTICE!**

If automatic discovery, rescan, add, or remove operations are in progress, you cannot rescan for a storage array.

2. Select **Tools < Rescan**.
3. In the confirmation dialog, click **OK** to start scanning the selected host for storage arrays. This process adds new storage arrays and updates the status of the old storage arrays that are connected to the selected host. Several minutes might elapse to complete the process.

9 Naming the Storage Array

9.1 Things to Know – Naming the Storage Array

- A storage array name can consist of letters, numbers, and the special characters underscore (_), hyphen (-), and pound sign (#). No other special characters are permitted.
- When you have named a storage array, the prefix "Storage Array" is automatically added to the name. For example, if you named the storage array "Engineering," it appears as "Storage Array Engineering."
- When you first discover a storage array or manually add it, the storage array will have a default name of "unnamed."

9.2 Procedure – Naming a Storage Array

1. From the **Setup** tab on the Enterprise Management Window, click **Name/Rename Storage Arrays**.
The **Name/Rename** dialog appears.
2. Perform one of these actions, depending on the number of unnamed storage arrays:
 - **More than one storage array is unnamed**
Go to step 3.
 - **One storage array is unnamed**
Go to step 6.
3. Select one of the unnamed storage arrays, and then select **Tools > Locate Storage Array**.
4. Find the physical storage array to make sure that you correlated it to the particular storage array listed.
5. Repeat step 3 through step 4 for each unnamed storage array.
6. Select an unnamed storage array in the top portion of the dialog.
The current name and any comment for the storage array appear at the bottom of the dialog.
7. Change the name of the storage array, add a comment (such as its location), and click **OK**.
The **Warning** dialog appears.
8. Perform one of these actions:
 - **The host is not running any path failover drivers**
Click **Yes** to change the name of the storage array. Go to step 9.
 - **The host is running a path failover driver**
Click **No**. Go to step 9.
9. Do you need to name other storage arrays?
 - **Yes**
Click **Apply** to make the change and to keep the dialog open. Go to step 3.
 - **No**
Click **OK** to make the change and to close the dialog.

10 Resolving Problems

If you noted any amber LEDs during Turning on the Power and Checking for Problems in the hardware installation documents, the Enterprise Management Window should show a corresponding indication.

10.1 Procedure – Resolving Problems

1. Click the **Devices** tab of the Enterprise Management Window to check the status of the storage arrays.
2. Double-click the storage array with the Needs Attention condition. The associated Array Management Window (AMW) is launched.
3. Click the **Physical** tab of the AMW to see the configuration.
4. Perform one of these actions, depending on the status shown:
 - **Optimal**
No problems need to be resolved. Go to *Section 11 Adding Controller Information for the Partially Managed Storage Array, page 49*
 - **Needs Attention**
Go to step 5.
 - **Unresponsive**
Refer to the online help topics in the Enterprise Management Window for the procedure.
5. Select **Storage Array**, and click **Recovery Guru** to launch the Recovery Guru. Follow the steps in the Recovery Guru.

10.2 Retrieving Trace Buffers

Use the **Advanced >>Troubleshooting >> Support Data >> Retrieve Trace Buffers** option to save trace information to a compressed file. The firmware uses the trace buffers to record processing, including exception conditions, that might be useful for debugging. Trace information is stored in the current buffer. You have the option to move the trace information to the flushed buffer after you retrieve the information. (The option to move the trace information to the flushed buffer is not available if you select **Flushed buffer** from the **Trace Buffers** list.) Because each controller has its own buffer, there might be more than one flushed buffer. You can retrieve trace buffers without interrupting the operation of the storage array and with minimal effect on performance.



NOTICE!

Use this option only under the guidance of your Customer and Technical Support representative.

A zip-compressed archive file is stored at the location you specify on the host. The archive contains trace files from one or both of the controllers in the storage array along with a descriptor file named `trace_description.xml`. Each trace file includes a header that identifies the file format to the analysis software used by the Customer and Technical Support representative.

The descriptor file has the following information:

- The World Wide Identifier (WWID) for the storage array.
- The serial number of each controller.
- A time stamp.
- The version number for the controller firmware.

- The version number for the management application programming interface (API).
 - The model ID for the controller board.
 - The collection status (success or failure) for each controller. (If the status is Failed, the reason for failure is noted, and no trace file exists for the failed controller.)
1. From the Array Management Window, select **Advanced > Troubleshooting > Support Data > Retrieve Trace Buffers**.
 2. Select the **Controller A** check box, the **Controller B** check box, or both check boxes. If the controller status message to the right of a check box is **Failed** or **Disabled**, the check box is disabled.
 3. From the **Trace Buffers** drop-down list, select **Current buffer**, **Flushed buffer**, **Current and flushed buffers**, or **Current, flushed, and platform buffers**.
 4. If you choose to move the buffer, select the **Move current trace buffer to the flushed buffer after retrieval** option.
The **Move current trace buffer to the flushed buffer after retrieval** option is not available if you selected **Flushed buffer** in step 3.
 5. In the **Specify filename** text box, either enter a name for the file to be saved (for example, C:\filename.zip), or browse to a previously saved file if you want to overwrite that file.
 6. Click **Start**.
The trace buffer information is archived to the file that you specified in step 5. If you click **Cancel** while the retrieval process is in progress, and then click **OK** in the cancellation dialog that appears, the trace buffer information is not archived, and the **Retrieve Trace Buffers** dialog remains open.
 7. When the retrieval process is finished, the label on the **Cancel** button changes to **Close**. Choose one of the following options:
 - To retrieve trace buffers again using different parameters, repeat step 2 through step 6.
 - To close the dialog and return to the Array Management Window, click **Close**.

11 Adding Controller Information for the Partially Managed Storage Array

**NOTICE!**

You only need to perform this step if you have partially managed storage arrays.

11.1 Key Terms

partially managed storage array

A condition that occurs when only one controller is defined or can be reached when the storage array is added to or found by the storage management software. In this case, volume management operations can be done only on volumes owned by the reachable controller. Many other management operations that require access to both controllers are not available.

11.2 Things to Know – Partially Managed Storage Arrays

You can identify a storage array as a partially managed storage array if you see these indications for the storage array:

- When you close the **Add New Storage Array – Manual** dialog after adding the storage array, a **Partially Managed Storage Arrays** dialog appears.
- When you try to manage the storage array using the Array Management Window, a **Partially Managed Storage Arrays** dialog appears.
- When you select **View Partially Managed Storage Arrays**, the storage array is listed in the **Partially Managed Storage Arrays** dialog.
- When you place the cursor on the storage array, “partially managed” appears in the tooltip.

Note:

The tooltip indication appears only for out-of-band storage arrays.

11.3 Procedure – Automatically Adding a Partially Managed Storage Array

**NOTICE!**

These steps are for out-of-band partially managed storage arrays only. For in-band partially managed storage arrays, verify the connection, and perform the steps in *Section 8.5 Procedure – Rescanning the Host for a New Storage Array, page 45*.

1. From the Enterprise Management Window, select **View Partially Managed Storage Arrays**.
2. Select the required partially managed storage array from the list of storage arrays.
3. Click **Add More** to add the information about the second controller.
The **Add New Storage Array – Manual** dialog appears.
4. Manually enter the host names or the IP addresses of the controllers (out-of-band management method) or the host name or IP address of the host running the host-agent software (in-band management method), and click **Add**.
The storage array appears in the Enterprise Management Window.

**NOTICE!**

You can enter IP addresses in either the IPv4 format or the IPv6 format.

**NOTICE!**

After adding the storage array, you can view or change the cache memory settings of the storage array (see *Section 16.4 Procedure – Changing the Cache Memory Settings, page 59*).

12 Manually Configuring the Controllers

This topic describes how you can manually configure the controllers in the storage array for out-of-band management.

12.1 Things to Know – Manually Configuring the Controllers



NOTICE!

You need to perform this step only if you want to use the out-of-band management method and you do not have a DHCP server to automatically assign IP addresses for the controllers.

- See *Section 3 Deciding on the Management Method, page 12* to determine if you need to make any configuration changes to the controller.
- In general, Ethernet port 1 on each controller is used for storage management, and Ethernet port 2 on each controller is used by the Customer and Technical Support representative.
- You should configure Ethernet port 2 only if your Customer and Technical Support representative asks you to do so.
- You can configure a gateway on only one of the Ethernet ports on each controller.
- Ethernet port 1 and Ethernet port 2 must be on different sub-networks.
- You can select one of the following speed and duplex mode combinations for your Ethernet ports. If you select the auto-negotiate option, the controller will use the highest speed supported by the Ethernet connection.

Table 12.1 Supported Speed and Duplex Mode Combinations

Speed	Duplex Mode
1000BASE-T	Duplex
1000BASE-T	Half-Duplex
100BASE-T	Duplex
100BASE-T	Half-Duplex
10BASE-T	Duplex
10BASE-T	Half-Duplex
Auto-negotiate	



NOTICE!

Your controller might not support some of the speed and duplex mode combinations. You can see the list of speed and duplex mode combinations that are supported on your controller when you change your network configuration. For the procedure to change your network configuration, see *Section 12.4 Procedure – Configuring the Controllers, page 52*.

12.2 Things to Know – Options for Manually Configuring the Controllers

If you will use the out-of-band method and do not have a DHCP server, you have two options for manually configuring your controllers.

Option 1 – Use the In-Band Management Method Initially (Recommended)

This option requires that you install the host-agent software on one of the hosts that is attached to the storage array and then use the in-band management method to initially discover the storage array and to manually configure the controllers. To discover the storage

array and to manually configure the controllers, perform the procedure in Procedure – Configuring the Controllers.

Option 2 – Set Up a Private Network



NOTICE!

This option is recommended only if the host on which you will use the in-band management method does not support the host-agent software.

This option requires that you install the storage management software on a management station (such as a laptop computer) and then set up a private network to initially discover the storage array and manually configure the controllers.

You can either connect your management station directly into Ethernet port 1 on each controller or use a hub (Ethernet switches or routers are not permitted).

To configure the management station, perform the procedure in Procedure – Configuring the Management Station.



NOTICE!

If you connect the management station directly to the Ethernet ports on the controller-drive tray other than a CE5400 controller-drive tray, you must use an Ethernet crossover cable. The Ethernet crossover cable is a special cable that reverses the pin contacts between the two ends of the cable.

12.3

Procedure – Configuring the Management Station

1. Change the IP address on the TCP/IP port on the management station from an automatic assignment to a manual assignment by using the default IP address subnet of the controllers.
 - Make note of the current IP address of the management station so that you can revert back to it after you have completed the procedure.
 - You must set the IP address for the management station to something other than the controller IP addresses (for example, use 192.168.128.100 for an IPv4 network, or use FE80:0000:0000:0000:02A0:B8FF:FE29:1D7C for an IPv6 network).

Note:

In an IPv4 network, the default IP addresses for Ethernet port 1 on controller A and controller B are 192.168.128.101 and 192.168.128.102, respectively.

- If your network is an IPv4 network, check the subnet mask to verify that it is set to 255.255.255.0, which is the default setting.
 - Refer to your operating system documentation for instructions about how to change the network settings on the management station and how to verify that the address has changed.
2. After you have configured your management station, perform the procedure in Procedure – Configuring the Controllers.

12.4

Procedure – Configuring the Controllers

1. In the **Devices** tab on the Enterprise Management Window, double-click the storage array for which you want to configure the controller network settings.
The associated Array Management Window is launched.
2. Click the **Physical** tab.
3. Highlight controller A in the Physical pane of the Array Management Window, and select **Controller > Configure > Ethernet Management Ports**.

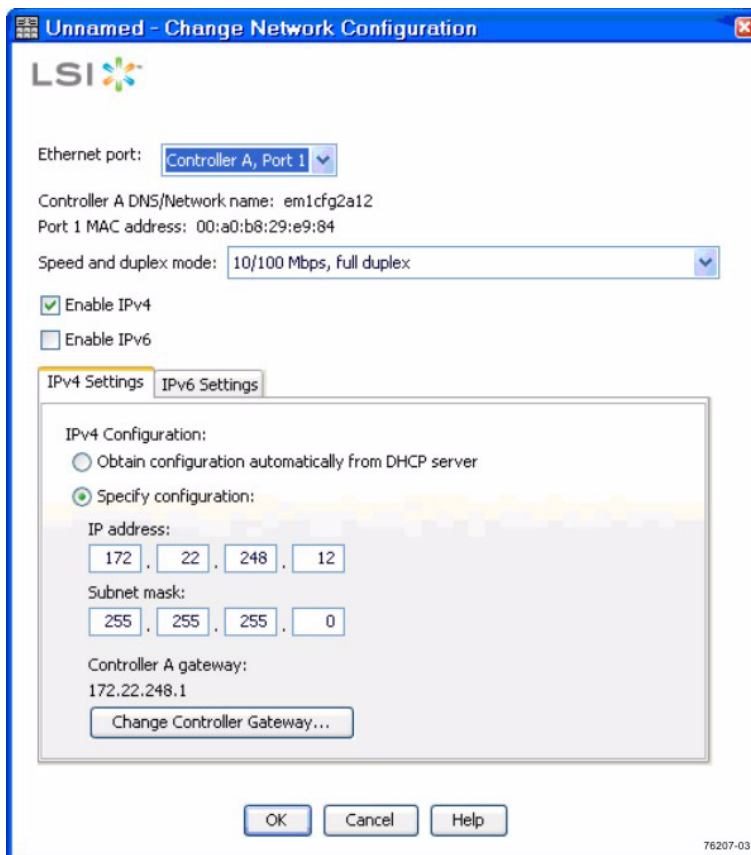


Figure 12.1 Change Network Configuration Dialog with IPv4 Settings

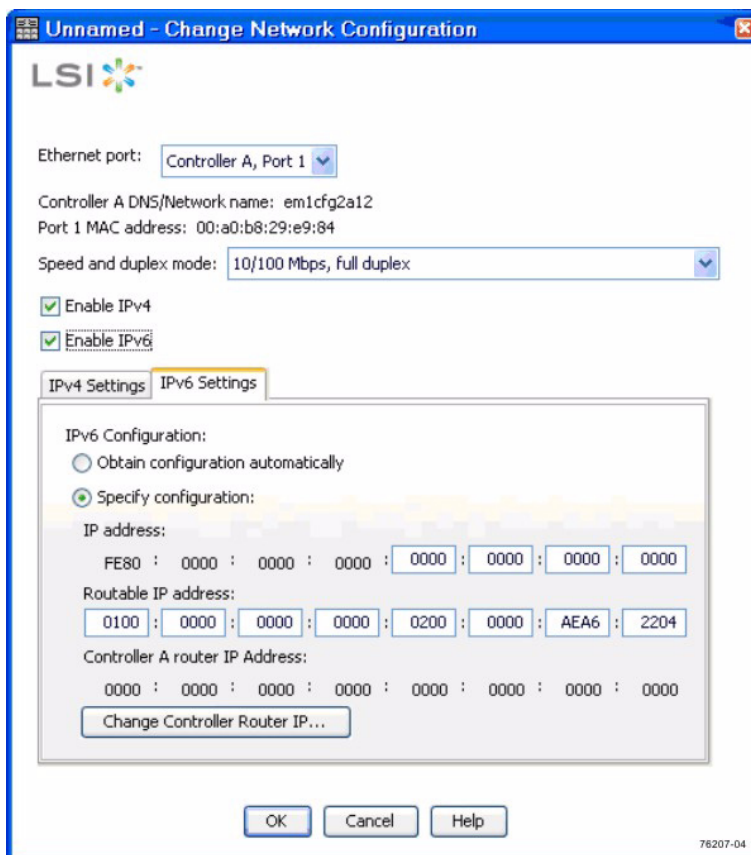


Figure 12.2 Change Network Configuration Dialog with IPv6 Settings

4. Select **Controller A, Port 1** in the **Ethernet port** drop-down list.
5. From the **Speed and duplex mode** drop-down list, select **Auto-negotiate**.



NOTICE!**Possible connectivity issues**

After you select Auto-negotiate, make sure that your Ethernet switch also is set to **Auto-negotiate**. Connectivity issues might occur if **Auto-negotiate** is not selected in SANtricity ES Storage Manager and is not set for the Ethernet switch.

-
6. Depending on the format of your network configuration information, select the **Enable IPv4** check box, the **Enable IPv6** check box, or both check boxes.
 7. Depending on the format that you have selected, enter the network configuration information (IP address, subnet mask, and gateway or IP address and routable IP address) in the **IPv4 Settings** tab or the **IPv6 Settings** tab.

Note:

You must obtain the network configuration information from your network administrator.

8. Select **Controller B, Port 1** in the **Ethernet port** drop-down list, and repeat step 5 through step 7 for controller B.
9. Click **OK**.
10. If you are manually configuring the controllers using a private network, perform these actions after configuring the controllers:
 - Disconnect the Ethernet cable from your management station, and reconnect the Ethernet cables from the controllers into your regular network.
 - Complete the steps necessary to change the management station's IP address back to what it was originally.

13 Setting a Password

13.1 Things to Know – Passwords

- You need to set a password for your storage array to protect it from serious damage, such as security breaches.
- When you set a password, only authorized personnel are allowed to run the commands that change the state of the storage array, such as commands to create volumes and the commands to modify the cache settings.
- For increased protection, use a long password with at least 15 alphanumeric characters. The maximum password length is 30 characters.
- Passwords are case sensitive.
- You will be asked for a password only when you first attempt to change the configuration (such as creating a volume) or when you first perform a destructive operation (such as deleting a volume). You must exit both the Array Management Window and the Enterprise Management Window to be asked for the password again.
- Any type of view operation does not require a password at any time.
- If you no longer want to have the storage array password-protected, enter the current password, and then leave the **New password** text box and the **Confirm password** text box blank.

**NOTICE!**

The storage array password is different from the pass phrase used for SafeStore Drive Security.

**NOTICE!**

If you forget your password, you must contact your Customer and Technical Support representative for help to reset it.

13.2 Procedure – Setting a Password

1. From the **Setup** tab on the Enterprise Management Window, click **Manage a Storage Array**.
The Select Storage Array dialog appears.
2. Highlight the storage array for which you want to set a password, and click **OK**.
The associated Array Management Window is launched.
3. From the **Setup** tab on the Array Management Window, click **Set a Storage Array Password**.
4. Follow the on-screen instructions. Click **Help** for more information.
5. Click **OK**.

14 Removing a Storage Array

14.1 Things to Know – Removing Storage Arrays

- When you remove a storage array, multiple storage arrays, or a host, they are removed from the Enterprise Management Window of your storage management station. They can be viewed from other storage management stations.
- You can delete the storage arrays and hosts from the Tree view or the Table view. These views are located on the **Devices** tab on the Enterprise Management Window. However, you can delete only one storage array at a time from the Tree view.

14.2 Procedure – Removing a Storage Array

Use these steps to remove a storage array, multiple storage arrays, or a host to which multiple storage arrays are connected.

1. From the Tree view or the Table view in the Enterprise Management Window **Devices** tab, select the storage array, the storage arrays, or the host that you want to remove.

**NOTICE!**

Before you try to remove a storage array, multiple storage arrays, or a host, you must close all of the Array Management Windows and the **Script Editor** dialogs that are associated with the selected storage arrays. If the Array Management Window or the **Script Editor** dialog is open for a storage array, that storage array is not removed. All of the other storage arrays are removed.

2. Select **Edit > Remove**.
3. In the confirmation dialog, click **Yes** to remove the storage array.
Depending on what you have selected to be removed, one of these actions occurs:
 - If you have selected a storage array, the storage array is removed from the Enterprise Management Window.
 - If you have selected multiple storage arrays, the storage arrays are removed from the Enterprise Management Window.
 - If you have selected a host, the host and its associated storage arrays are removed from the Enterprise Management Window.

**NOTICE!**

While removing multiple storage arrays, multiple confirmation dialogs, one for each storage array, appear.

15 Configuring Email Alerts and SNMP Alerts

This topic describes how you can make sure that SANtricity ES Storage Manager sends critical issues with the storage array to the correct email address.

15.1 Key Terms

Management Information Base (MIB)

CONTEXT [Management] The specification and formal description of a set of objects and variables that can be read and possibly written using the Simple Network Management Protocol (SNMP). (The Dictionary of Storage Networking Terminology, 2004)

Simple Network Management Protocol (SNMP)

CONTEXT [Network] [Standards] An IETF protocol for monitoring and managing systems and devices in a network. The data being monitored and managed is defined by a Management Information Base (MIB). The functions supported by the protocol are the request and retrieval of data, the setting or writing of data, and traps that signal the occurrence of events. (The Dictionary of Storage Networking Terminology)

15.2 Things to Know – Alert Notifications

- Setting alert destinations lets you specify addresses for the delivery of email messages and SNMP trap messages whenever a critical problem exists with the storage array.
- You must have the Event Monitor running on a machine (a management station or a host) to receive alerts. The machine should be one that runs continuously.



NOTICE!

If you choose not to automatically enable the event monitor during installation, you do not receive critical alert notifications.

15.3 Procedure – Setting Alert Notifications

1. From the **Setup** tab on the Enterprise Management Window, click **Configure Alerts**. The **Select Storage Array** dialog appears.
2. Indicate on which storage arrays you want the alerts to be set, and click **OK**.
 - If you selected the **All Storage Arrays** choice, the main **Alerts** dialog appears.
 - If you selected the **Individual Storage Array** choice, you must first select the specific storage array and click **OK** before the main **Alerts** dialog appears.
 - If you selected the **Specific Host** choice, you must first select a host and click **OK** before the main **Alerts** dialog appears.

3. Specify the alerts that you want by using the tabs on the dialog. Use this information, and click **OK** when you are finished setting the alerts.

Mail Server Tab

- You must specify a mail server and an email sender address if you want to set email alerts. The mail server and sender address are not required if you are setting SNMP alerts.
- The Sender Contact Information is optional. Include the information if you plan to send alerts to your Customer and Technical Support representative; otherwise, delete the fields.

Email Tab

- Enter the email addresses in standard format, such as `xxx@company.com`.
- If one of the email alerts that you configure is for your Customer and Technical Support representative, make sure that you select the **Event + Profile** or **Event + Support** choice in the Information to Send column. This additional information aids in troubleshooting your storage array. The **Event + Support** choice includes the profile.

SNMP Tab

- To set up alert notifications using SNMP traps, you must copy and compile a Management Information Base (MIB) file on the designated network management station.
- The SNMP trap destination is the IP address or the host name of a station running an SNMP service. At a minimum, this destination will be the network management station.

16 Changing the Cache Memory Settings

This topic provides information about modifying cache memory settings in your storage array through the SANtricity ES Storage Manager to enhance system performance.

16.1 Key Terms

cache memory

An area of random access memory (RAM) on the controller. This memory is dedicated to collecting and holding related data until a drive tray or a storage tray is ready to process the data. Cache memory has a faster access time than the actual drive media.

16.2 Things to Know – Cache Memory Settings

- If the data requested from the host for a read exists in the cache memory from a previous operation, the drive is not accessed. The requested data is read from the cache memory.
- Write data is written initially to the cache memory. When a percentage of unwritten data is reached, the data is flushed from or written to the drives.
- During a controller failure, the data in the cache memory of the controller might be lost.
- To protect data in the cache memory, you can set a low percentage of unwritten data in the cache memory to trigger a flush to the drives. However, as the number of drive reads and drive writes increases, this setting decreases performance.
- When cache mirroring is enabled, if one controller in a controller tray or controller-drive tray fails, the second controller takes over. The surviving controller uses its mirrored version of the failed controller's cache data to continue reading from and writing to the volumes previously managed by the failed controller.

16.3 Procedure – Viewing the Cache Memory Size Information

1. From the **Setup** tab on the Enterprise Management Window, click **Manage a Storage Array**.
The **Select Storage Array** dialog appears.
2. Select the storage array that you want to manage, and click **OK**.
The associated Array Management Window is launched.
3. Click the **Physical** tab.
4. Select controller A in the Physical pane of the Array Management Window, and the **Properties** view appears in the left pane.
5. Scroll through the **Base** tab until you find the cache information and the cache backup device information.

16.4 Procedure – Changing the Cache Memory Settings

1. From the **Setup** tab on the Enterprise Management Window, click **Manage a Storage Array**.
The **Select Storage Array** dialog appears.
2. Select the storage array that you want to manage, and click **OK**.
The associated Array Management Window is launched.
3. Select **Storage Array ChangeCache Settings**.
The associated **Change Cache Settings** dialog appears.
4. Select the percentage of unwritten data in the cache to trigger a cache flush in the **Start flushing** text box.

5. Select the percentage of unwritten data in the cache to stop a cache flush in progress in the **Stop flushing** text box.
6. Select the required cache block size, and click **OK**.

16.5

Procedure – Changing the Volume Cache Memory Settings

1. From the **Setup** tab on the Enterprise Management Window, click **Manage a Storage Array**.
The **Select Storage Array** dialog appears.
2. Select the storage array you want to manage, and click **OK**.
The associated Array Management Window is launched.
3. Select **Volume > Change > Cache Settings**.
The associated **Change Cache Settings** dialog appears.
4. To allow read operations from the host to be stored in the cache memory, select the **Enable read caching** check box.
5. To allow write operations from the host to be stored in the cache memory, select the **Enable write caching** check box.
6. Select the enable write caching options by using the information in this list:
 - **Enable write caching without batteries** – Allows data from the drives to be written to the cache memory even when the controller batteries are discharged completely, not fully charged, or not present.
 - **Enable write caching with mirroring** – Mirrors data in the cache memory across two redundant controllers that have the same cache memory size.
7. To enable copying of additional data while copying read operations data from the drives, select the **Dynamic cache read prefetch** check box.
8. Click **OK**.

17 Enabling the Premium Features

Note:

If you did not obtain any premium feature key files from your storage vendor, skip this step.

17.1 Key Terms

premium feature

A feature that is not available in the standard configuration of the storage management software.

17.2 Things to Know – Premium Features

You enable a premium feature through a feature key file that you obtain from your storage vendor. The premium feature is either enabled or disabled. When a premium feature is disabled, it does not appear in the graphical user interface (GUI).

If your system is a low-tier performance configuration and you want to upgrade to a high-tier performance configuration, use the following procedure to obtain enhanced performance.

17.3 Procedure – Enabling the Premium Features

1. From the **Setup** tab on the Enterprise Management Window, click **Manage a Storage Array**.
The **Select Storage Array** dialog appears.
2. Highlight the storage array on which you want to enable a premium feature, and click **OK**.
The associated Array Management Window appears.
3. Select **Storage Array > Premium Features**.
The associated **Premium Features and Feature Pack Information** dialog appears.
4. Select a feature from the **Premium Feature** list.
5. Click **Enable**.
The associated **Select Feature Key File** dialog appears.
6. Enter the file name of the feature key file for the particular premium feature that you want to enable.
7. Click **OK** to close the **Select Feature Key File** dialog.
The **Premium Features installed on storage array** drop-down list shows the name and the status of the premium feature that you have enabled.
8. Repeat step 4 through step 7 for each premium feature that you want to enable.

18 Defining the Hosts

Note:

- You must know the world wide port names of each HBA host port. If you have not already recorded them, see *Section 6 Configuring the Host Bus Adapters, page 30* for your particular configuration (E2600 Controller-Drive Tray) for instructions to obtain these world wide port names.
- If you will not use storage partitions or you do not have the SANshare Storage Partitioning premium feature enabled on your storage array, you can skip the information about *Section 18.2 Things to Know – Host Groups, page 62* and *Section 18.3 Things to Know – Storage Partitions, page 62*, and go to either *Section 18.4 Procedure – Defining the Hosts, page 65* or *Section 18.5 Procedure – Defining the iSCSI Hosts, page 65*.

18.1 Things to Know – Hosts

The host adapters in the hosts that are attached to the storage array are known to the storage management software. However, the storage management software does not know which host adapters are associated with which hosts. Use these steps to associate each host with its specific host adapters.

18.2 Things to Know – Host Groups

- A host group is a group (cluster) of two or more hosts that share access, in a storage partition, to specific volumes on the storage array. You can create an optional logical entity in the storage management software. You must create a host group only if you will use storage partitions.
- If you must define a host group, you can define it through the Define Hosts Wizard described in *Procedure – Defining the Hosts*.

18.3 Things to Know – Storage Partitions

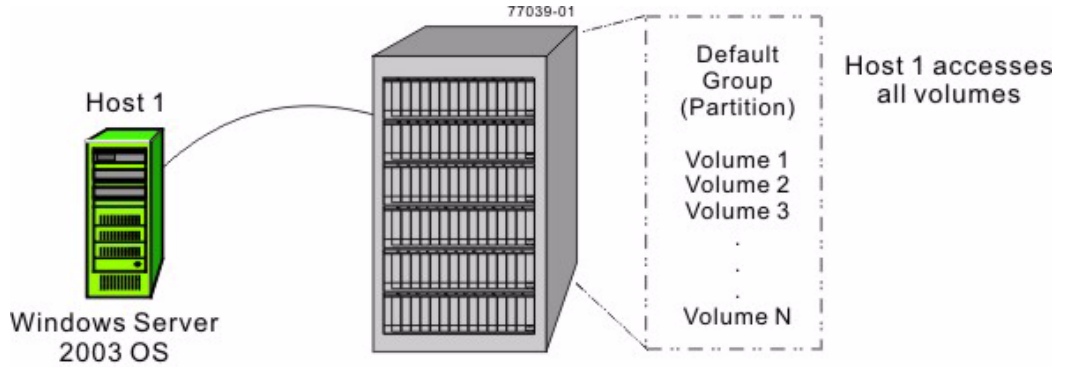
- A storage partition is a logical entity that consists of one or more volumes that can be accessed by a single host or can be shared among hosts that are part of a host group. You can think of a storage partition as a virtual storage array. That is, take the physical storage array and divide it up into multiple virtual storage arrays that you can then restrict to be accessible only by certain hosts.
- SANshare Storage Partitioning is a premium feature. This premium feature was either already enabled on your storage array at the factory, or you must purchase a feature key file from your storage vendor to enable it.
- You do not create storage partitions in this step, but you must understand them to define your hosts.
- You do not need to create storage partitions if these conditions exist (see *Figure 18.1*):
 - You have only one attached host that accesses all of the volumes on the storage array.
 - You plan to have all of the attached hosts share access to all of the volumes in the storage array.

Note:

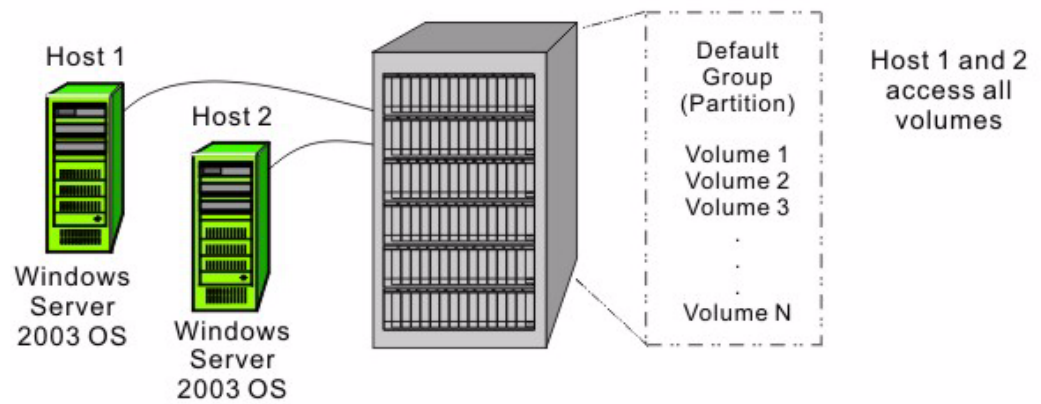
All of the attached hosts must have the same operating system (homogeneous), and you must have special software on the hosts (such as clustering software) to manage volume sharing and accessibility. This qualification does not, however, exclude the use of heterogeneous hosts (see *Figure 18.3*).

- You do need to create storage partitions if these conditions exist (see *Figure 18.1*):
 - You want certain hosts to access only certain volumes.
 - You have hosts with different operating systems (heterogeneous) attached in the same storage array. You must create a storage partition for each type of host.

Example of No Additional Storage Partitions Required



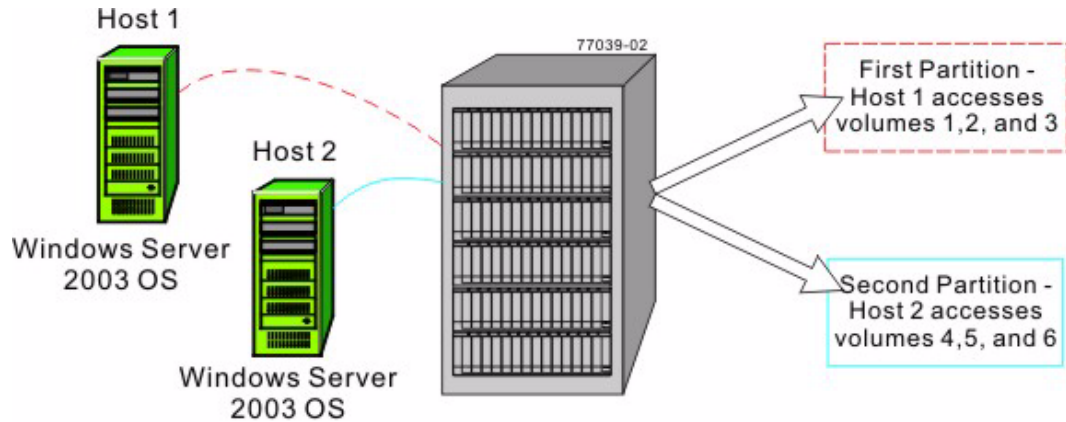
A single host accesses **all** volumes; **no** additional storage partitions are needed.



Multiple homogeneous hosts share access to **all** volumes; **no** additional storage partitions are needed and **no** specific host group is needed.

Figure 18.1 Example of No Additional Storage Partitions Required

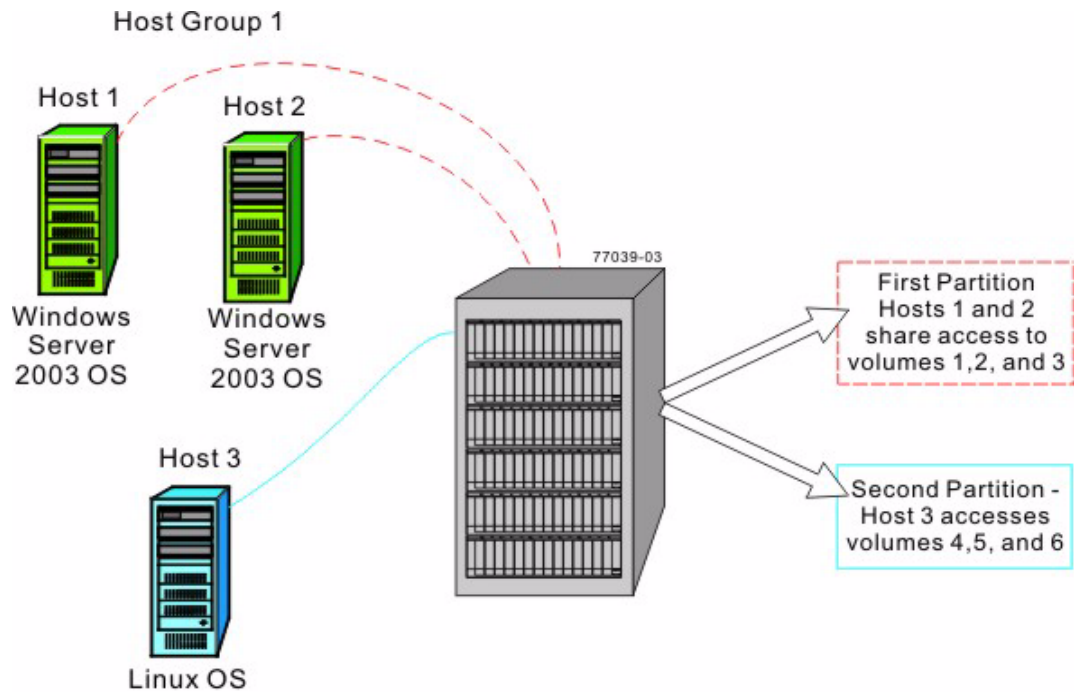
Example of Additional Storage Partitions Required (Homogeneous Host)



- Each host needs access to specific volumes.
- Both hosts use the same operating system (homogeneous).
- Storage divided into two logical storage partitions.
- A Default Group (partition) is not used.

Figure 18.2 Example of Additional Storage Partitions Required (Homogeneous Host)

Example of Additional Storage Partitions Required (Heterogeneous Hosts)



- Host 1 and host 2 (Windows Server 2003 OS) share access to specific volumes through host group 1.
- Two heterogeneous hosts (Linux OS and Windows Server 2003 OS) exist.
- Host 3 (Linux) accesses specific volumes.
- Storage is divided into two logical storage partitions.
- A Default Group (partition) is not used.

Figure 18.3 Example of Additional Storage Partitions Required (Heterogeneous Hosts)

18.4 Procedure – Defining the Hosts

1. From the **Setup** tab on the Enterprise Management Window, click **Manage a Storage Array**.
The **Select Storage Array** dialog appears.
2. Highlight the storage array on which you want to define a host, and click **OK**.
The associated Array Management Window is launched.
3. From the **Setup** tab on the Array Management Window, click **Manually Define Hosts**.
4. Use the on-screen instructions and the online help topics to define your hosts and associate the HBA host ports. This procedure also allows you to define a host group.

18.5 Procedure – Defining the iSCSI Hosts

1. From the **Setup** tab on the Enterprise Management Window, click **Manage a Storage Array**.
The **Select Storage Array** dialog appears.
2. Highlight the storage array on which you want to define a host, and click **OK**.
The associated Array Management Window is launched.
3. From the **Setup** tab on the Array Management Window, click **Configure iSCSI Host Ports**.
4. On the **Configure Ethernet port speed** drop-down list, select either **10 Gbps** or **1 Gbps** to set the port speed to either 10 Gb/s or 1 Gb/s. By default, this value is set to **10 Gbps**.
5. Use the on-screen instructions and the online help topics to further define your hosts and associate the HBA host ports. This procedure also allows you to define a host group.

19 Configuring the Storage

This topic describes how you can group and manage your storage within the storage array for maximum efficiency.

19.1 Key Terms

Default Group

A standard node to which all host groups, hosts, and host ports that do not have any specific mappings are assigned. The standard node shares access to any volumes that were automatically assigned default logical unit numbers (LUNs) by the controller firmware during volume creation.

free capacity

Unassigned space in a volume group that can be used to make a volume.

full disk encryption (FDE)

A type of drive technology that can encrypt all data being written to its disk media.

hot spare drive

A spare drive that contains no data and that acts as a standby in case a drive fails in a RAID Level 1, RAID Level 3, RAID Level 5, or RAID Level 6 volume. The hot spare drive can replace the failed drive in the volume.

Redundant Array of Independent Disks (RAID)

CONTEXT [Storage System] A disk array in which part of the physical storage capacity is used to store redundant information about user data stored on the remainder of the storage capacity. The redundant information enables regeneration of user data in the event that one of the array's member disks or the access path to it fails. Although it does not conform to this definition, disk striping is often referred to as RAID (RAID Level 0). (The Dictionary of Storage Networking Terminology)

storage partition

A logical entity that is made up of one or more storage array volumes. These storage array volumes can be accessed by a single host or can be shared with hosts that can be part of a host group.

unconfigured capacity

The available space on drives of a storage array that has not been assigned to a volume group.

volume

The logical component created for the host to access storage on the storage array. A volume is created from the capacity available on a volume group. Although a volume might consist of more than one drive, a volume appears as one logical component to the host.

volume group

A set of drives that is logically grouped and assigned a RAID level. Each volume group created provides the overall capacity needed to create one or more volumes.

19.2 Things to Know – Data Assurance

The Data Assurance (DA) premium feature checks for and corrects errors that might occur as data is communicated between a host and a storage array. DA is implemented using the SCSI direct-access block-device protection information model. DA creates error-checking information, such as cyclic redundancy checks (CRCs) and appends that information to each

block of data. Any errors that might occur when a block of data is either transmitted or stored are then detected and corrected by checking the data with its error-checking information. Only certain configurations of hardware, including DA-capable drives, controllers, and host interface cards (HICs), support the DA premium feature. When you install the DA premium feature on a storage array, SANtricity ES Storage Manager provides options to use DA with certain operations. For example, you can create a volume group that includes DA-capable drives, and then create a volume within that volume group that is DA-enabled. Other operations that use a DA-enabled volume have options to support the DA premium feature. If you choose to create a DA-capable volume group, select the **Create a Data Assurance (DA) capable volume group** check box. This check box is enabled only when there is at least one DA-capable drive in the storage array and is, by default, selected if it is enabled. When the DA premium feature is enabled, the DA Enabled column appears in the **Source volume** list in the **Create Copy Wizard – Introduction** dialog. If you choose to copy a DA-enabled source volume to a target volume that is not DA enabled, you are prompted to confirm your choice. The copy can be completed, but the resulting copy is not DA enabled.



NOTICE!

If a volume group is DA-capable and contains a DA-enabled volume, use only DA-capable drives for hot spare coverage. A volume group that is not DA capable cannot include a DA-enabled volume.

You can verify that a drive contains DA-enabled volumes by checking that the **Data Assurance (DA) capable** property is set to **yes**.

19.3

Things to Know – Allocating Capacity

- You can create volumes from either unconfigured capacity or free capacity on an existing volume group.
 - If you create a volume from unconfigured capacity, you must first specify the parameters for a new volume group (RAID level and capacity for a set of drives) before you specify the parameters for the first volume on the new volume group.
 - If you create a volume from free capacity, you have to specify the parameters of only the volume, because the volume group already exists.
- As you configure the capacity on the storage array, make sure that you leave some unassigned drives available. You might need to use these drives for these reasons:
 - To create additional volume groups for new capacity requirements
 - For hot spare drive protection
 - To increase the free capacity on an existing volume group to provide for future capacity needs
 - For additional storage required for certain premium features, such as Snapshot Volume
- If your storage array contains more than one type of drive (such as Fibre Channel or SATA), an Unconfigured Capacity node will be associated with each drive type. You cannot mix drives of different types within the same volume group.
- If you are adding capacity to a Data Assurance (DA) -capable volume group, use only drives that are DA capable. If you add a drive or drives that are not DA-capable, the volume group no longer has DA capabilities, and you no longer have the option to enable DA on newly created volumes within the volume group. The DA Capable column in the **Available drives** list shows the DA capabilities of each listed drive.
- If you are adding capacity to a volume group that is not DA capable, do not use drives that are DA capable because the volume group will not be able to take advantage of the

capabilities of DA-capable drives. The DA Capable column in the **Available drives** list shows the DA capabilities of each listed drive.

19.4 Things to Know – Volume Groups and Volumes

- You can create a single volume or multiple volumes per volume group. Usually, you will create more than one volume per volume group to address different data needs or because of limits on the maximum capacity of a single volume.
Note:
If you choose to copy a Data Assurance (DA)-enabled source volume to a target volume that is not DA enabled, you are prompted to confirm your choice. The copy can be completed, but the resulting copy is not DA enabled. For more information about how volume copy is affected by DA-enabled volumes, refer to *Volume Copy Premium Feature* electronic document topics.
- While creating volume groups, you must make sure that the drives that comprise the volume group are located in different drive trays. This method of creating volume groups is called tray loss protection. Tray loss protection guarantees accessibility to the data on the volumes in a volume group if a total loss of communication occurs with a single drive tray. Communication loss might occur due to loss of power to the drive tray or failure of the drive tray ESMs.
- The RAID levels supported are RAID Level 0, RAID Level 1, RAID Level 3, RAID Level 5, RAID Level 6, and RAID Level 10 (1 + 0).
 - RAID Level 0 provides no data redundancy.
 - RAID Level 10 is not a separate RAID level choice but is supported when you create a RAID Level 1 volume group that consists of four or more drives.
 - You can assign RAID Level 1 only to volume groups with an even number of drives.
 - You can assign RAID Level 3 or RAID Level 5 only to volume groups with three or more drives.
 - You can assign RAID Level 6 only to volume groups with five or more drives.

Note:

RAID Level 6 is a premium feature. This premium feature was either already enabled on your storage array at the factory, or you must purchase a feature key file from your storage vendor to enable it.

19.5 Things to Know – Host-to-Volume Mappings and Storage Partitions

- Each volume that you create must be mapped to a logical address called a logical unit number (LUN). The host uses this address to access data on the volume.
- When you create a volume manually, you have two choices for mapping:
 - **Default mapping**
Choose this option if you do not intend to use storage partitions. The storage management software will automatically assign a LUN to the volume and make the volume available to all of the hosts that are attached to the storage array in the Default Group (partition).
 - **Map later (assign specific mapping)**
Choose this option if you intend to use storage partitions. Use the Define Storage Partition Wizard to indicate the host group or host, specify the volumes that you want the host group or host to access, and access the LUNs to assign to each volume.

19.6 Things to Know – Hot Spare Drives

- The hot spare drive adds a level of redundancy to your storage array. It is highly recommended that you create hot spare drives for each type of drive in your storage array.
- Hot spare drives do not provide protection for RAID Level 0 volume groups because data redundancy does not exist on these volume groups.
- A hot spare drive is not dedicated to a specific volume group but instead is global, which means that a hot spare drive will be used for any failed drive in the storage array. The failed drive must be the same drive type and have a capacity that is equal to or smaller than the particular hot spare drive.

19.7 Things to Know – Full Disk Encryption

SafeStore Drive Security and SafeStore Enterprise Key Manager (EKM) are premium features that prevent unauthorized access to the data on a drive that is physically removed from the storage array. Controllers in the storage array have a security key. Secure drives provide access to data only through a controller that has the correct security key. The security key can be managed locally by the controllers or externally by an external key management server, which is the EKM premium feature. Both SafeStore Drive Security and EKM must be enabled either by you or your storage vendor.

The SafeStore Drive Security premium feature requires security-capable full disk encryption (FDE) drives. A security-capable FDE drive encrypts data during writes and decrypts data during reads. Each security-capable drive has a unique drive encryption key.

When you create a secure volume group from security-capable FDE drives, the drives in that volume group become security enabled. When a security-capable FDE drive has been security enabled, the drive requires the correct security key from a controller to read or write the data. All of the drives and controllers in a storage array share the same security key. The shared security key provides read and write access to the drives, while the drive encryption key on each drive is used to encrypt the data. A FDE drive works like any other drive until it is security enabled.

Whenever the power is turned off and turned on again or is removed from the controller-drive tray, all of the FDE drives change to a security locked state. In this state, the data is inaccessible until the correct security key is provided by a controller.

You can view the SafeStore Drive Security status of any drive in the storage array from the **Drive Properties** dialog. The status information reports whether the drive is:

- Security-capable
- Secure – Security enabled or disabled
- Read/Write Accessible – Security locked or unlocked

You can view the security status of any volume group in the storage array from the **Volume Group Properties** dialog. The status information reports whether the storage array is one of the following:

- Security-capable
- Secure

The following table shows how to interpret the security properties status of a volume group.

Table 19.1 Volume Group Security Properties

	Security-Capable – Yes	Security-Capable – No
Secure – Yes	The volume group is composed of all FDE drives and is in a Secure state.	Not applicable. Only FDE drives can be in a Secure state.
Secure – No	The volume group is composed of all FDE drives and is in a Non-Secure state.	The volume group is not entirely composed of FDE drives.

When the SafeStore Drive Security premium feature has been enabled, the **Drive Security** menu appears in the **Storage Array** menu.

The **Drive Security** menu has these options:

- **Create Security Key**
- **Change Security Key**
- **Save Security Key**
- **Unlock Drives**

**NOTICE!**

If you have not created a security key for the storage array, only the Create Security Key option is active.

If you have created a security key for the storage array, the Create Security Key option is inactive with a check mark to the left. The Change Security Key option and the Save Security Key options are now active.

The **Unlock Drives** option is active if any security-locked drives exist in the storage array. When the SafeStore Drive Security premium feature has been enabled, the **Secure Drives** option appears in the **Volume Group** menu. The **Secure Drives** option is active if these conditions are true:

- The selected storage array is not security enabled but is composed entirely of security-capable drives.
- The storage array contains no snapshot base volumes or snapshot repository volumes.
- The volume group is in Optimal status.
- A security key is set up for the storage array.

The **Secure Drives** option is inactive if the previous conditions are not true.

The **Secure Drives** option is inactive with a check mark to the left if the volume group is already security enabled.

You can erase security-enabled drives instantly and permanently so that you can reuse the drives in another volume group or in another storage array. You can also erase them if the drives are being decommissioned. When you erase security-enabled drives, the data on that drive becomes permanently inaccessible and cannot be read. When all of the drives that you have selected in the Physical pane are security enabled, and none of the selected drives is part of a volume group, the **Secure Erase** option appears in the **Drive** menu.

The storage array password protects a storage array from potentially destructive operations by unauthorized users. The storage array password is independent from the SafeStore Drive Security premium feature and should not be confused with the pass phrase that is used to protect copies of a SafeStore Drive Security security key. However, it is good practice to set a storage array password before you create, change, or save a SafeStore Drive Security security key or unlock secure drives.

19.8 Procedure – Configuring the Storage

1. From the **Setup** tab on the Enterprise Management Window, click **Manage a Storage Array**.
The **Select Storage Array** dialog appears.
2. Highlight the storage array on which you want to configure storage, and click **OK**.
The associated Array Management Window is launched.
3. From the **Setup** tab on the Array Management Window, click **Configure Storage Array**.
4. Choose the applicable configuration task:
 - **Automatic configuration**
This method creates volume groups with equal-sized capacity volumes and also automatically assigns appropriate hot spare drive protection. Use this method if you do not have unique capacity requirements for each volume or you want a quick method to configure volume groups, volumes, and hot spare drives. You can choose from a list of suggested configurations, or you can create your own custom configuration.
 - **Create volume groups and volumes**
This method creates one volume at a time but gives you more control over the volume group and volume parameters (such as RAID level, volume group, volume capacity, and so on). Use this method if you have unique capacity requirements for most of the volumes that you will create and you want more control in specifying various parameters.
 - **Configure hot spare drives**
This method lets you either have the software automatically assign applicable hot spare protection (which is identical to the automatic configuration method described previously) or manually create a hot spare drive from an unassigned drive that you select.
5. To create the volume groups, volumes, and hot spare drives, perform one of these actions depending on your storage partition requirements. Refer to the on-screen instructions and the online help topics for more information.
 - **No storage partition is required, and you selected the automatic configuration method**
Go to step 6.
 - **No storage partition is required, and you selected the manual configuration method**
Verify whether all volumes are mapped to the Default Group, and go to step 8.
 - **A storage partition is required**
Go to step 7.
6. Perform these actions:
 - From the **Setup** tab on the Array Management Window, click **Map Volumes**.
 - Select the Default Group, and assign each volume a logical unit number (LUN).
 - Go to step 8.

Note:

To map all volumes into the Default Group, you must select the **Default Mapping** option while creating the volumes.

7. Perform these actions:
 - Click the **Mappings** tab.
 - Specify the applicable host or host group, volumes, and LUNs.
 - Select **Mappings > Define**, and click **SANshare Storage Partitioning**.
 - Refer to the on-screen instructions.
 - Repeat the same for each storage partition.
 - Go to step 8.
8. After you have created all of the volumes and mappings, use the applicable procedures on your hosts to register the volumes and to make them available to your operating system.
 - Depending on your operating system, two utilities are included with the storage management software (hot_add and SMdevices). These utilities help register the volumes with the hosts and also show the applicable device names for the volumes.
 - You also will need to use specific tools and options that are provided with your operating system to make the volumes available (that is, assign drive letters, create mount points, and so on). Refer to your host operating system documentation for details.
 - If you are using the HP-UX OS, you must run this command on each host to change the I/O timeout value to 120 seconds on each block device (volume) that you created on the storage array, where `cxtxdx` is the device name of each volume.

```
pvchange -t 120 /dev/dsk/cxtxdx
```

Note:

If you reboot your host, you must run the `pvchange` command again.

Note:

After you configure the volume, you can change the cache memory settings of the volume (see *Section 16.4 Procedure – Changing the Cache Memory Settings, page 59*).

20 Downloading the Drive and ATA Translator Firmware for SATA Drives

Each SATA drive in a DE6900 drive tray is connected to a corresponding ATA translator (12 to a drawer). The ATA translator provides Fibre Channel (FC) protocol to Serial Advanced Technology Attachment (SATA) protocol translation for the SATA drives in the storage array. Use the **Drive/ATA Translator Firmware** option to transfer a downloadable firmware file to the drives and the Advanced Technology Attachment (ATA) translators in the storage array only if the drives and the ATA translators in the storage array are experiencing firmware-related limitations or performance issues. Obtain drive and ATA translator firmware only from your storage supplier.

You can download firmware files to multiple drives and ATA translators at a time to keep downtime to a minimum.

**NOTICE!****Risk of application errors**

Stop all I/O activity to the storage array before downloading the firmware to prevent application errors. Before starting any firmware download, make sure that all data on the affected drives is backed up.

Keep these important guidelines in mind when you download firmware to avoid the risk of application errors:

- Downloading firmware incorrectly could result in damage to the drives or loss of data. Perform downloads only under the guidance of your Customer and Technical Support representative.
 - Stop all I/O to the storage array before the download.
 - Make sure that the firmware that you download to the drives and the ATA translators is compatible with the drives and the ATA translators that you select.
 - Do not make any configuration changes to the storage array while downloading the firmware.
-

CAUTION!**Possible loss of data**

Perform downloads only under the guidance of your Customer and Technical Support representative. Downloading firmware files incorrectly could result in performance problems or loss of data.

CAUTION!**Possible damage to drives and loss of data**

Do not make any configuration changes to the storage array while downloading firmware files.

**NOTICE!**

Before you download firmware to all of the drives, and the ATA translators in the storage array, consider downloading to just a few drives and ATA translators to make sure that the downloads are successful and to test the performance of the new firmware. When you are satisfied that the new firmware works correctly, download the firmware to the remaining drives and ATA translators.

**NOTICE!**

Downloads can take several minutes to complete. During a download, the **Download Drive and ATA Translator - Progress** dialog appears. Do not attempt another operation when the **Download Drive and ATA Translator - Progress** dialog is shown.

1. From the Array Management Window, select **Advanced MaintenanceDownloadDrive/ATA Translator Firmware**.
The **Download Drive and ATA Translator Firmware - Introduction** dialog appears.
2. Follow the directions on each dialog, and click **Next** to move to the next dialog.
Each dialog has context-sensitive help. Click **Help** to view the information applicable for that particular dialog.

20.1 Things to Know – A Preview of the Download Drive and ATA Translator Firmware Dialog

Table 20.1 Preview of Dialogs

Dialog	Description
Download Drive and ATA Translator Firmware Wizard – Introduction	Provides information about downloading the firmware to the drives and the ATA translators.
Download Drive and ATA Translator Firmware Wizard – Select Packages	Lets you select the firmware for the drives and the ATA translators.
Download Drive and ATA Translator Firmware Wizard – Select Services	Lest you select the drives and the ATA translators that you want to update with the previously selected firmware.
Download Drive and ATA Translator Firmware Wizard – Download Progress	Lets you monitor the progress of the firmware download.

20.2 Procedure – Starting the Download Process

The **Download Drive and ATA Translator Firmware - Introduction** dialog is the first dialog of the Download Drive and ATA Translator Firmware Wizard that downloads drive and Advanced Technology Attachment (ATA) translator firmware to one or more drives and ATA translators in the storage array.

1. Review the information in the dialog to determine whether you are ready to download the firmware.
2. To continue with the firmware download process, click **Next**.

20.3 Procedure – Selecting the Drive and the ATA Translator Firmware

Use the **Download Drive and ATA Translator Firmware - Select Packages** dialog to select the drive and Advanced Technology Attachment (ATA) translator firmware that you want to download.

1. To open the dialog to select the firmware, click **Add**, and navigate to the directory that contains the files that you want to download.
2. Select up to four firmware files.

Note:

Selecting more than one firmware file to update the firmware of the same drive or ATA translator might result in a file-conflict error. If a file-conflict error occurs, an error dialog appears. To resolve this error, click **OK**, and remove all other firmware files except the

one that you want to use for updating the firmware of the drive or the ATA translator. To remove a firmware file, select the firmware file in the Selected packages area, and click **Remove**.

3. To move to the next dialog, click **Next**.

20.4 Procedure – Updating the Firmware

Use the **Download Drive and ATA Translator Firmware - Select Devices** dialog to select the drives and the Advanced Technology Attachment (ATA) translators that you want to update with the previously selected firmware. The selected firmware for the drive appears in the Drive firmware information area. The selected firmware for the ATA translator appears in the ATA translator firmware information area. If you must change the firmware, click **Back** to return to the previous dialog.

1. Select the drives and ATA translators for which you want to download the firmware.
 - **For one or more drives and ATA translators** – In the Select devices area, select the drive and ATA translator names.
 - **For all compatible drives and ATA translators listed in the dialog** – Click **Select All**.
2. Click **Finish**.

The **Confirm Download** dialog appears.
3. To start the firmware download, type *yes* in the text box.
4. Click **OK**.

20.5 Procedure – Monitoring the Progress of the Download

Use the **Download Drive and ATA Translator Firmware - Progress** dialog to monitor the progress of the drive and the Advanced Technology Attachment (ATA) translator firmware download.

CAUTION!

Possible loss of access to data or data loss

Stopping a firmware download might result in drive unavailability or data loss.

1. Monitor the progress of the drive and the ATA translator firmware download. The progress and status of each drive and each ATA translator that are participating in the download appears in the Progress column of the Devices updated area and in the Progress summary area.

Note:

- Each firmware download can take several minutes to complete.
 - A drive or an ATA translator does not show in the Devices updated area until a firmware download is attempted or the firmware download process is stopped.
2. To stop the firmware download in progress, click **Stop**.

Any firmware downloads currently in progress are completed. Any drives or ATA translators that have attempted firmware downloads show their individual status. Any remaining drives or ATA translators are listed with a status of Not attempted.
 3. If you want to save a text report of the progress summary, click **Save As**.

The report saves with a default `.txt` file extension. If you want to change the file extension or directory, change the parameters in the **Save As** dialog.
 4. Perform one of these actions:
 - **To close the Drive Firmware Download Wizard** – Click **Close**.
 - **To start the wizard again** – Click **Transfer More**.

Table 20.2 Status of Drives and ATA Translators

Status Shown	Definition
Scheduled	The firmware download has not yet started.
In progress	The firmware is being transferred to the drive or the ATA translator.
Failed - partial	The firmware was only partially transferred to the drive before a problem prevented the rest of the file from being transferred.
Failed - invalid state	The firmware is not valid.
Failed - other	The firmware could not be downloaded, possibly because of a physical problem with the drive or the ATA translator.
Not attempted	The firmware was not downloaded. The download was stopped before it could occur.
Successful	The firmware was downloaded successfully.

21 Restrictions

This section lists Controller Firmware, Host Software, and Third-party Component restrictions

- Force Volume Group Import Operation Fails when Started Immediately after a Drive is Removed (see *Page 77*)
- Bosch Configuration Manager Does Not Support Saving Changes for Maximum Number of Cameras (400) (see *Page 78*)
- Bosch Cameras Timeout When Removing a Drive with I/O (Hot Pull) and Intermittently Timeout When Failing a Reconstructing Drive (see *Page 78*)
- No Warning in Management Software for Stopping Host I/O Before Starting ESM Firmware Download on Simplex System (see *Page 78*)
- Cache Data Loss in Simplex System After Reboot If Volume Cache Mirroring Was Enabled During Cache Block Size Change (see *Page 79*)
- Attempts to Initialize Foreign Drive Fail (see *Page 79*)
- Drive Channel Summary Dialog Does Not Show that Interface Link Rates in the Drive Channel Are Operating at a Different Speeds (see *Page 80*)
- Replacement of a Cache Backup Device Is Not Correctly Logged (see *Page 80*)
- With Missing Drives During Start-of-Day, Cache Restore Did Not Occur (see *Page 81*)
- Delay between a Mouse or Keyboard Command and Updating the Array Management Window User Interface (see *Page 82*)
- SMcli Scripts That Export Multiple Volume Groups with Large Drive Counts Fail (see *Page 83*)
- During Start-of-Day Initialization a Controller Is Held Offline Due to Multi-Bit Error Correcting Code Errors (see *Page 83*)
- Force Volume Group Import Operation Fails when Started Immediately after a Drive is Removed (see *Page 84*)

Force Volume Group Import Operation Fails when Started Immediately after a Drive is Removed

Operating System	All operating systems
Hardware/Software/ Firmware	<ul style="list-style-type: none"> – All controllers – SANtricity ES Storage Manager Version 10.80 and earlier
Problem or Restriction	This problem occurs when a drive is removed prior to starting a Force Volume Group Import operation on the volume group which the drive belongs to. The Force Volume Group Import operation issued by the management software client may timeout with Return Code 404 (RETCODE_VOLUME_GROUP_STATE_NOT_VALID). However, the operation should complete successfully.
Workaround	To avoid this problem, do not remove a drive prior to starting a Force Volume Group Import operation on the volume group which the removed drive belongs to. If a drive must be removed before starting a Force Volume Group Import operation, wait 5 minutes after reinserting the drive before starting the operation. If this problem occurs, retry the Force Volume Group Import operation or refresh the SANtricity client managing the array.

Bosch Configuration Manager Does Not Support Saving Changes for Maximum Number of Cameras (400)

Operating System	All operating systems
Hardware/Software/Firmware	Bosch Configuration Manager application (version 04.32.0014.0) managing 400 camera devices
Problem or Restriction	This problem occurs with the Bosch Configuration Manager application when managing 400 camera devices. When attempting to assign the devices to a target port or modifying device parameters for all 400 devices, the command is unsuccessful in updating all devices and may return an error. Only 200 of the 400 camera devices are updated.
Workaround	To avoid this problem, perform the operation by selecting only 200 camera devices at a time.

Bosch Cameras Timeout When Removing a Drive with I/O (Hot Pull) and Intermittently Timeout When Failing a Reconstructing Drive

Operating System	All operating systems
Hardware/Software/Firmware	<ul style="list-style-type: none"> – 26xx controller platform – Bosch Camera version 5.52.5 – Bosch Video Recording Manager version 02.21.0027
Problem or Restriction	The Host I/O timeout for the Bosch cameras is 10 seconds and the Bosch Video Recording Manager application is 5 seconds. When removing a drive that is not failed during host I/O, the host I/O's will timeout since the recovery time to detect the removed SAS drive, transition the affected volumes to Degraded mode, and complete processing of the I/O's exceeds the timeout thresholds. When the preferred method of failing the drive before removal is followed, the operation completes within the camera timeout thresholds. For the operation of failing a drive that is performing reconstruction, the camera I/O's will intermittently timeout due to I/Os being suspended during the configuration operations of stopping Reconstruction, failing the drive, and transitioning the volumes back to Degraded mode.
Workaround	To avoid this problem, drives should be failed before removing them.

No Warning in Management Software for Stopping Host I/O Before Starting ESM Firmware Download on Simplex System

Operating System	All operating systems
Hardware/Software/Firmware	Simplex controller configuration

Problem or Restriction	During the ESM firmware download operation on a Simplex system, all host I/O needs to be stopped since there is only a single drive-side path to the expansion enclosures and drives. The Management Software does not provide a dialog to remind the user that I/O needs to be stopped before performing the operation.
Workaround	The user needs to stop I/O from all hosts including the camera devices, Video Recording Manager (VRM), and Archive Player applications. Follow the provided Simplex ESM firmware download procedure.

Cache Data Loss in Simplex System After Reboot If Volume Cache Mirroring Was Enabled During Cache Block Size Change

Operating System	All operating systems
Hardware/Software/Firmware	Simplex controller configuration
Problem or Restriction	This problem occurs on a Simplex system if cache mirroring is enabled on any of the volumes when the array cache block size is changed. If this sequence of operations occurs, there may be a cache data loss condition when the controller is rebooted. If the cache block size for the storage array is changed when cache mirroring is not enabled on any of the volumes, the condition is resolved and cache data loss will not occur after a reboot. In a Simplex environment, the user should not enable cache mirroring, since it will internally disable both write caching and cache mirroring since there is not a second controller to support mirroring. The default cache mirroring setting for new volume creation is disabled in the NVSRAM, so the end user would have to manually enable cache mirroring.
Workaround	To avoid this problem, do not enable cache mirroring on any volumes in a Simplex system.

Attempts to Initialize Foreign Drive Fail

Operating System	All operating systems
Hardware/Software/Firmware	Controller firmware version 7.80

Problem or Restriction	This problem occurs when a drive is migrated between storage systems and then returned to the original storage system. When a drive that was configured with one storage system is migrated and configured to another storage system and then migrated back to the original storage system, the drive contains volume group configuration information for both the source and the migration storage systems. The drive is locked out and cannot be initialized to clear the lockout condition.
Workaround	To avoid this problem, initialize the drive on the foreign storage system before migrating the drive into another storage system. Caution: Potential loss of data – Reinitializing the drive can cause data loss.

Drive Channel Summary Dialog Does Not Show that Interface Link Rates in the Drive Channel Are Operating at a Different Speeds

Operating System	All operating systems
Hardware/Software/ Firmware	<ul style="list-style-type: none"> – SANtricity ES Storage Manager Version 10.80 – All versions of SANtricity ES Storage Manager that support platforms with SAS channels
Problem or Restriction	<p>This problem occurs when the local interface link rate and the shared interface link rate in a SAS drive channel operate at different speeds. When the interface link rates are operating at different speeds, SANtricity ES Storage Manager shows the controller's local interface rate as the drive channel link rate. The drive channel summary dialog might show that the drive channel is operating at the correct speed.</p> <p>When one drive channel interface is operating at a lower link rate than the other drive channel interface, MEL event 0x1717 is logged, and the MEL description is <code>Link in the array controller enclosure is slow</code>. The Logged by field in the MEL shows which controller logged the MEL event.</p>
Workaround	To recover from this problem, contact your Customer and Technical Support representative for instructions on how to analyze the problem and repair the affected component or replace the affected component.

Replacement of a Cache Backup Device Is Not Correctly Logged

Operating System	All operating systems
Hardware/Software/ Firmware	All controllers

Problem or Restriction	<p>This problem occurs when one of the following events occurs when either the storage system has only a single slot for each controller for a cache backup device, or the storage array has multiple slots for each controller, but only one slot contains a cache backup device.</p> <ul style="list-style-type: none"> - The last available cache backup device is removed or replaced. - Vibrations or loose placements cause the device to lose contact with the slot. - The device was not correctly seated in the slot. <p>MEL event message 0x7504, which indicates that the cache backup device was replaced, is not logged. When removing the device reduces the cache backup capacity, Recovery Guru event 0x211F is logged to indicate that the total capacity of the cache backup device was not satisfied.</p>
Workaround	<p>To avoid this problem, make sure that the replacement cache backup device is correctly inserted in the slot, that the device has contact with the slot, and the that device is correctly seated in the slot.</p> <p>To recover from this problem, follow the instructions in the Recovery Guru.</p>

With Missing Drives During Start-of-Day, Cache Restore Did Not Occur

Operating System	All operating systems
Hardware/Software/Firmware	Controller firmware version 7.80
Problem or Restriction	<p>This problem occurs during start-of-day (SOD) when all of the following conditions exist:</p> <ul style="list-style-type: none"> - There were host I/Os until either a reboot or power cycle previously stopped the controller. - During SOD, one or more drives are missing from the previous reboot. - The volumes are configured either as write-through or as write back cache and cache mirroring is disabled. <p>When the I/Os occur on a missing drive, the pieces associated with that drive fail, and the drive stays in the Missing state. The volumes associated with the failed pieces might also fail or be degraded, depending on the redundancy available.</p>
Effect on Cache Restore process	<p>The Restore process cannot restore the backed-up data for a volume when the volume is in a Failed state, so the Restore process that starts during Restore SOD after the controllers reboot might not complete.</p>

Effect on Interrupted Write Recovery Process	Failed volumes that have interrupted writes recorded and preserved in NVSRAM during the previous reboot cycle lose those interrupted writes as those interrupted write records are cleared upon volume failure.
Workaround	<p>To avoid this problem take the following actions:</p> <ul style="list-style-type: none"> – Restrict all internal I/Os from occurring on missing drives. – To avoid Interrupted Write Recovery errors, set all volume cache properties to Write back cache and Cache mirroring enabled. To minimize data integrity loss caused by interrupted write problems, configure volumes as write-through and enable Tray Loss Protection during the volume creation process. – To reduce the potential for failed or degraded volume, set the cache setting as Write Through. Write through volumes will stay that way until they are manually revived. – After a power cycle, make sure that the drive trays are started first, and then the controllers are started. – To prevent interrupted writes and data corruption, make sure Cache mirroring is enabled for volumes that have Write back cache enabled. – To prevent failed pieces and failed volumes, make sure that drives and drive trays that are part of RAID volumes are not missing during SOD. <p>To recover from this problem, reinsert drives and start them. The drive returns to an Optimal state, but the failed pieces and the failed volumes associated with the drive stay in a Failed state. Although the drive returns to an Optimal state, some loss of data integrity is possible even when no pieces or volumes are failed.</p> <p>Note: When the SOD occurs because of a power cycle, volumes stay in a Failed state, and the Restore process does not complete.</p>

Delay between a Mouse or Keyboard Command and Updating the Array Management Window User Interface

Operating System	All Linux operating system
Hardware/Software/ Firmware	<ul style="list-style-type: none"> – SANtricity ES Storage Manager Version 10.80 – X11
Problem or Restriction	This problem occurs when SANtricity ES Storage Manager Version 10.80 is used on the Linux OS with X11, such as SSH with XManager in an xterm session. SANtricity's painting logic causes multiple repaints for some user interface components, which results in a delayed update of the Array Management Window (AMW).
Workaround	To avoid this problem, manage the storage array locally, and do not use SANtricity ES Storage Manager with X11.

SMcli Scripts That Export Multiple Volume Groups with Large Drive Counts Fail

Operating System	All operating systems
Hardware/Software/ Firmware	SMcli script
Problem or Restriction	<p>This problem occurs when an SMcli script tries to export multiple volume groups that contain large numbers of drives. The first export operation causes an internal controller to rediscover the exported volume group. The first export command succeeds and returns a good status back to the SMcli.</p> <ul style="list-style-type: none"> – The rediscovery operation is independent of the SMcli script. Rediscovery enables the exported volume group to be re-imported into the original source array without having to pull or push the drives. – Rediscovery requires the controller translock and takes about 7 seconds for each drive in the volume group. <p>To perform its export, the second volume group export command from the SMcli also requires the controller translock, so the second volume group export command waits for the first translock to end. But the second SMcli command times out after 180 seconds. The SMcli retries the second volume group export command again after 180 seconds, but if a third volume group export is already in progress, the retried second volume group export command fails with a 400 or 404 error status.</p>
Workaround	To avoid this problem, do not use the same SMcli script to perform consecutive multiple exports of volume groups that contain large numbers of drives. To use an SMcli script for exporting volume groups, create separate scripts for running the exports, and wait several minutes before running consecutive exports. To recover from this problem, run the failed SMcli script commands again.

During Start-of-Day Initialization a Controller Is Held Offline Due to Multi-Bit Error Correcting Code Errors

Operating System	All operating systems
Hardware/Software/ Firmware	E2600 controller-drive trays
Problem or Restriction	If one or more multi-bit error correction code (ECC) errors occur at the start of RAID parity assist (RPA), the controller enters into a reboot loop during start-of-day initialization. Eventually the controller will enter hardware lockdown and display diagnostic errors on the 7-segment LED display.
Workaround	Contact customer support for diagnosis and recovery procedure.

Force Volume Group Import Operation Fails when Started Immediately after a Drive is Removed

Operating System	All operating systems
Hardware/Software/ Firmware	<ul style="list-style-type: none">– All Controllers– SANtricity ES Storage Manager Version 10.80 and earlier
Problem or Restriction	This problem occurs when a drive is removed prior to starting a Force Volume Group Import operation on the volume group which the drive belongs to. The Force Volume Group Import operation issued by the management software client may timeout with Return Code 404 (RETCODE_VOLUME_GROUP_STATE_NOT_VALID). However, the operation should complete successfully.
Workaround	To avoid this problem, do not remove a drive prior to starting a Force Volume Group Import operation on the volume group which the removed drive belongs to. If a drive must be removed before starting a Force Volume Group Import operation, wait 5 minutes after reinserting the drive before starting the operation. If this problem occurs, retry the Force Volume Group Import operation or refresh the SANtricity client managing the array.

Bosch Security Systems

Werner-von-Siemens-Ring 10
85630 Grasbrunn
Germany

www.boschsecurity.com

© Bosch Security Systems, 2012