



Initial Configuration and Software Installation for SANtricity ES[®] Storage Manager

Version 10.77

May 2011

51340-00, Rev. A



Revision History

Version and Date	Description of Changes
51340-00, Rev. A May 2011	Initial release of the document.

LSI and the LSI & Design logo, StorageTek, SANtricity, HotScale, and SANshare are trademarks or registered trademarks of LSI Corporation or its subsidiaries or Sun Microsystems, Inc. All other brand and product names may be trademarks of their respective companies.

This document contains proprietary information of LSI Corporation and Sun Microsystems, Inc. The information contained herein is not to be used by or disclosed to third parties without the express written permission of an officer of LSI or Sun.

It is the policy of LSI and Sun to improve products as new technology, components, software, and firmware become available. We reserve the right to make changes to any products herein at any time without notice. All features, functions, and operations described herein may not be marketed in all parts of the world. In some instances, photographs and figures are of equipment prototypes. Therefore, before using this document, consult your sales representative or account team for information that is applicable and current. WE DO NOT ASSUME ANY RESPONSIBILITY OR LIABILITY FOR THE USE OF ANY PRODUCTS DESCRIBED HEREIN EXCEPT AS EXPRESSLY AGREED TO IN WRITING BY LSI .

LSI products are not intended for use in life-support appliances, devices, or systems. Use of any LSI product in such applications without written consent of the appropriate LSI officer is prohibited.

LSI Corporate Headquarters
Milpitas, CA
800-372-2447

Email
globalsupport@lsi.com

Website
www.lsi.com

Document Number: 51340-00, Rev. A
Copyright © 2011 LSI Corporation. All rights reserved.
Copyright © 2011 Sun Microsystems, Inc. All rights reserved.

Table of Contents

Step 1 – Deciding on the Management Method	1
Key Terms	1
access volume	1
Dynamic Host Configuration Protocol (DHCP)	1
in-band management	1
out-of-band management	1
stateless address autoconfiguration	1
World Wide Identifier (WWID)	2
Procedure – Deciding on the Management Method	2
Things to Know – In-Band and Out-of-Band Requirements	4
Step 2 – Setting Up the Storage Array for Windows Server 2008 Server Core	5
Procedure – Configuring the Network Interfaces	5
Procedure – Setting the iSCSI Initiator Services	6
Procedure – Installing the Storage Management Software	6
Procedure – Configuring the iSCSI Ports	7
Procedure – Configuring and Viewing the Targets	7
Procedure – Establishing a Persistent Login to a Target	8
Procedure – Verifying Your iSCSI Configuration	8
Procedure – Reviewing Other Useful iSCSI Commands	8
Procedure – Configuring Your Storage Array	9
Step 3 – Installing the SANtricity ES Storage Manager Software	10
Key Terms	10
host	10
monitor	10
multi-path driver	10
Redundant Dual Active Controller (RDAC) multi-path driver	10
storage management station	10
Things to Know – All Operating Systems	10
Things to Know – Specific Operating Systems	11
Things to Know – System Requirements	11
Procedure – Installing the SANtricity ES Storage Manager Software	13
Things to Know – Software Packages	14
Procedure – Manually Installing RDAC on the Linux OS	17
Step 4 – Configuring the Host Bus Adapters	18
Procedure – Configuring the HBAs	18
Procedure – Changing the Emulex HBA Driver Configuration (Linux OS)	19
Procedure – Changing the Emulex HBA Driver Configuration (Solaris OS)	19
Procedure – Changing the Emulex HBA Driver Configuration (Windows Server 2003 OS and Windows Server 2008 OS)	20
Procedure – Changing the QLogic HBA Configuration (BIOS Settings)	20
Procedure – Changing the QLogic HBA Configuration (Solaris OS)	21
Procedure – Changing the QLogic HBA Configuration (Windows Server 2003 OS and Windows Server 2008 OS)	22
Step 5 – Starting SANtricity ES Storage Manager	23
For Additional Information	23
Procedure – Starting SANtricity ES Storage Manager	23
Things to Know – Enterprise Management Window and Array Management Window	24

Step 6 – Adding the Storage Array	26
Things to Know – Storage Array	26
Procedure – Automatically Adding a Storage Array	26
Procedure – Manually Adding a Storage Array	26
Things to Know – Rescanning the Host for a New Storage Array	28
Procedure – Rescanning the Host for a New Storage Array	28
Step 7 – Naming the Storage Array	29
Things to Know – Naming the Storage Array	29
Procedure – Naming a Storage Array	29
Step 8 – Resolving Problems	30
Procedure – Resolving Problems	30
Things to Know – Support Monitor Profiler	30
Procedure – Retrieving Trace Buffers	31
Step 9 – Adding Controller Information for the Partially Managed Storage Array	32
Key Terms	32
partially managed storage array	32
Things to Know – Partially Managed Storage Arrays	32
Procedure – Automatically Adding a Partially-Managed Storage Array	32
Step 10 – Manually Configuring the Controllers	34
Things to Know – Manually Configuring the Controllers	34
Things to Know – Options for Manually Configuring the Controllers	34
Option 1 – Use the In-Band Management Method Initially (Recommended)	34
Option 2 – Set Up a Private Network	35
Procedure – Configuring the Management Station	35
Procedure – Configuring the Controllers	35
Step 11 – Setting a Password	39
Things to Know – Passwords	39
Procedure – Setting a Password	39
Step 12 – Removing a Storage Array	40
Things to Know – Removing Storage Arrays	40
Procedure – Removing a Storage Array	40
Step 13 – Configuring Email Alerts and SNMP Alerts	41
Key Terms	41
Management Information Base (MIB)	41
Simple Network Management Protocol (SNMP)	41
Things to Know – Alert Notifications	41
Procedure – Setting Alert Notifications	41
Step 14 – Changing the Cache Memory Settings	43
Key Terms	43
cache memory	43
Things to Know – Cache Memory Settings	43
Procedure – Viewing the Cache Memory Size Information	43
Procedure – Changing the Cache Memory Settings	43
Procedure – Changing the Volume Cache Memory Settings	44
Step 15 – Enabling the Premium Features	45
Key Terms	45
premium feature	45

Things to Know – Premium Features	45
Procedure – Enabling the Premium Features	45
Step 16 – Defining the Hosts	46
Things to Know – Hosts	46
Things to Know – Host Groups	46
Things to Know – Storage Domains	46
Procedure – Defining the Hosts	48
Procedure – Defining the iSCSI Hosts	48
Step 17 – Configuring the Storage	50
Key Terms	50
Default Group	50
free capacity	50
full disk encryption (FDE)	50
hot spare drive	50
Redundant Array of Independent Disks (RAID)	50
storage domain	50
unconfigured capacity	50
volume	51
pool	51
Things to Know – T10 Protection Information	51
Things to Know – Allocating Capacity	51
Things to Know – Pools and Volumes	52
Things to Know – Host-to-Volume Mappings and Storage Domains	52
Things to Know – Hot Spare Drives	53
Things to Know – Encryption Services	53
Procedure – Configuring the Storage	54
Step 18 – Downloading the Drive and ATA Translator Firmware for SATA Drives and the DE6900 Drive Module	57
Procedure – Starting the Download Process	58
Procedure – Selecting the Drive and the ATA Translator Firmware	58
Procedure – Updating the Firmware	58
Procedure – Monitoring the Progress of the Download	59

Step 1 – Deciding on the Management Method

This document describes the decisions necessary for installing and starting SANtricity ES Storage Manager for Version 10.77, 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 6580/6780 controller module, the ST2500 M2 array module, CDE2600-60 array module, or the 6180 array module.

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 software, connect the cables, and use the storage management software.

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*)

Procedure – Deciding on the 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 [Step 10 – Manually Configuring the Controllers](#) 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

Figure 1 In-Band Management Topology

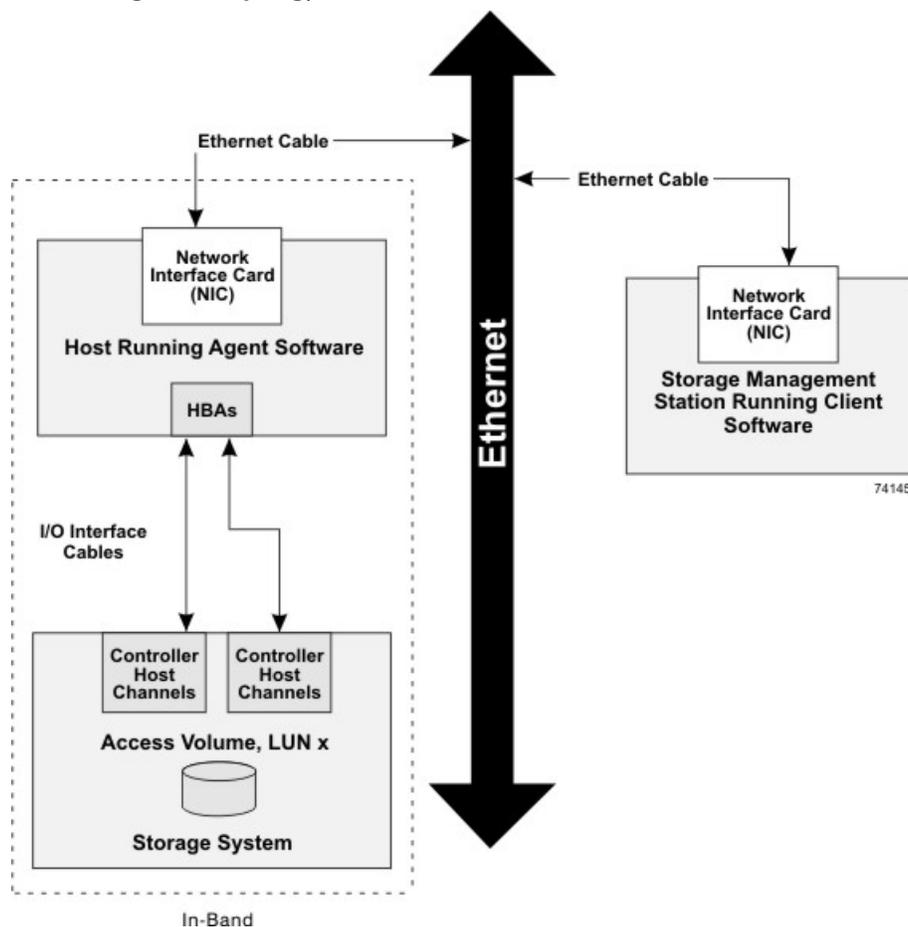
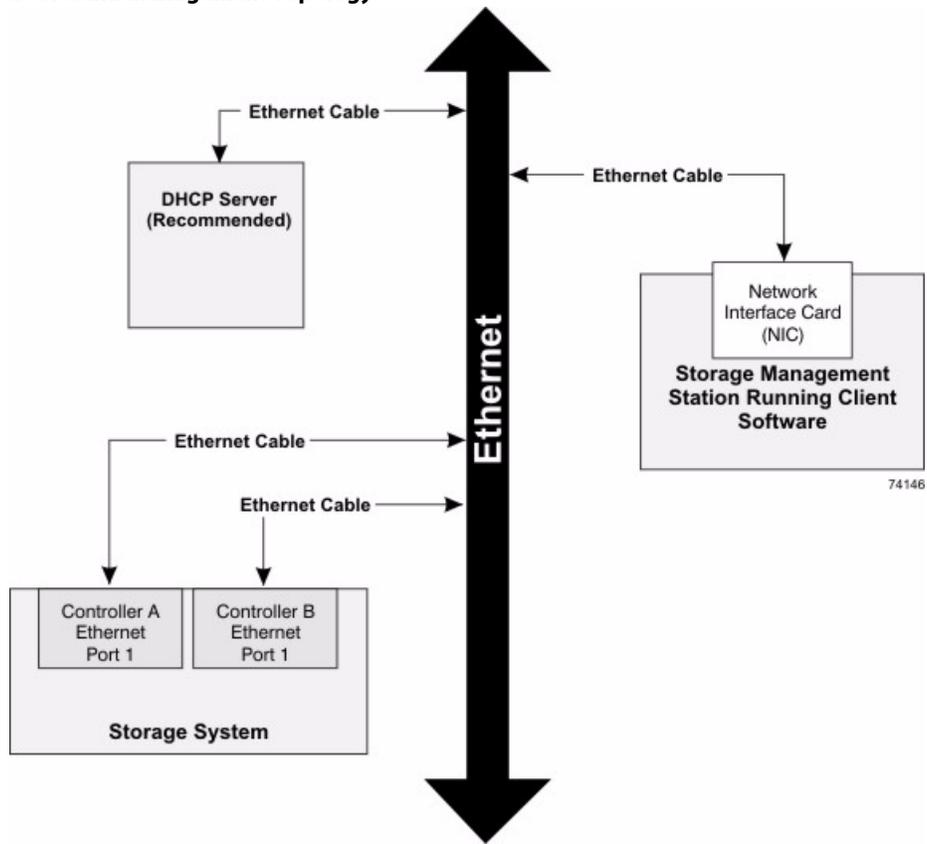
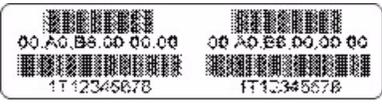


Figure 2 Out-of-Band Management Topology



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

Table 1 Out-of-Band and In-Band Management Requirements

Management Method	Requirements	Advantages	Disadvantages
Out-of-band <i>without</i> a DHCP server	<p>Connect separate Ethernet cables to each controller.</p> <p>Manually configure the network settings on the controllers. See “Manually Configuring the Controllers” for more information.</p>	<p>This method does not use a logical unit number (LUN) on the host.</p> <p>You do not need to install the host-agent software.</p> <p>This method does not use the SAS, Fibre Channel, or iSCSI bandwidth for storage array management functions.</p>	<p>You must manually configure the network settings on the controllers.</p> <p>Ethernet cables are required.</p>
Out-of-band – IPv6 stateless address auto-configuration <i>without</i> a DHCP server (IPv6 networks only)	<p>Connect separate Ethernet cables to each controller.</p> <p>Connect at least one router for sending the IPv6 network address prefix in the form of router advertisements.</p>	<p>No additional manual network configuration is required on the controllers.</p> <p>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 array module.</p> <p>You do not need to install host-agent software.</p> <p>This method does not use a LUN on the host.</p> <p>This method does not use the Fibre Channel or iSCSI bandwidth for storage array management functions.</p>	<p>Ethernet cables are required.</p>
Out-of-band <i>with</i> a DHCP server (IPv4 networks only)	<p>Connect separate Ethernet cables to each controller.</p> <p>Assign either static IP addresses or dynamic IP addresses to the controllers. It is recommended that you assign static IP addresses.</p> <p>Check your DHCP server for the IP addresses that are associated with the media access control (MAC) addresses of the controllers.</p> <p>The MAC address appears on a label on each controller in the form: xx.xx.xx.xx.xx.xx.</p> 	<p>No additional manual network configuration is required on the controllers.</p> <p>By default, the controllers automatically obtain their IP addresses from the DHCP server after you turn on the power to the array module.</p> <p>You do not need to install host-agent software.</p> <p>This method does not use a LUN on the host.</p> <p>This method does not use the Fibre Channel or iSCSI bandwidth for storage array management functions.</p>	<p>Ethernet cables are required.</p>
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.</p> <p>This method requires a special access volume to communicate. This volume is created automatically.</p>	<p>No additional manual network configuration is required on the controller.</p>	<p>This method uses a LUN on the host.</p> <p>This method uses the Fibre Channel bandwidth for storage array management functions.</p>

Step 2 – 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 [Step 3 – Installing the SANtricity ES Storage Manager Software](#).

If your host is running Windows Server 2008 Server Core, you must use the command line to install and configure your storage array.

If you are using Fibre Channel host connections, perform these procedures:

1. Install the storage management software using [Step 3 – Installing the SANtricity ES Storage Manager Software](#).
2. Configure your storage array using [Step 17 – Configuring the Storage](#).

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.
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.

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:

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

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 these commands, <IPv6 address> is the IPv6 address for the iSCSI initiator.

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.

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 Sun Customer Care Center 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 Sun Customer Care Center 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.

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 either the *Command Line Interface and Script Commands for Version 10.77* electronic document topics or the PDF on the SANtricity ES Storage Manager Installation DVD 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.

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. If you are *not* using CHAP, type this command for each port on the target from the command line:

```
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.

2. If you *are* using CHAP, type this command for each port on the target from the command line:

```
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.

3. 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.

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.

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.

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*.

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. Go to [Step 17 – Configuring the Storage](#) to finish configuring your storage array.
- You also can configure the storage array using the command line interface. Refer to Configuring a Storage Array in the *Configuring and Maintaining a Storage Array Using the Command Line* electronic document topic or on the PDF on the SANtricity ES Storage Manager Installation DVD for information that will help you configure your storage array.

Step 3 – 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 [Step 2 – Setting Up the Storage Array for Windows Server 2008 Server Core](#). If you are not running Windows Server 2008u Server Core, begin with the following tasks.

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.

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, and the Solaris OS, the storage management software supports using the storage array as a boot device. For assistance with setting up this configuration, contact your Sun Customer Care Center representative.

NOTE 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.

Things to Know – Specific Operating Systems

Solaris OS:

- The Solaris OS supports the use of the LSI Redundant Disk Array Controller (RDAC) multi-path driver for failover if the number of data volumes is less than or equal to 32. For systems with more than 32 data volumes, use 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 and Support Monitor packages 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) Storage Management Initiative (SMI) are not supported on these operating systems.

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

- 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 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.
- These operating systems support the use of the SteelEye® LifeKeeper, Novell Open Enterprise Server (OES), and Native Red Hat Clustering software for clustering.

Things to Know – System Requirements

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

Table 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	Standard Server Edition system (32-bit and 64-bit) Standard Enterprise Edition, (32-bit and 64-bit) x64 Edition (for AMD and EM64T support) x86-based system (AMD64 and EM64T)
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.
Windows Server 2008 and Windows Server Virtualization	x86-based system (AMD64 and EM64T) Standard (Server Core) Edition, Enterprise (Server Core) Edition, Web Edition
Macintosh OS X	10.5.8 10.6.3
Linux	IA32 AMD64 EM64T Red Hat Enterprise Linux 6.0 Red Hat Enterprise Linux 5.6 SUSE Linux Enterprise Server 10 SP 3 SUSE Linux Enterprise Server 11 SP1 Red Hat 5.0 Client (storage management stations only) SUSE Linux Enterprise Server 10, SP 3 (storage management stations only)
HP-UX	IA64 PA-RISC 11.31
AIX	Power PC processor 6.1, 7.1
Solaris	SPARC-based system x86-based system (Intel Xeon, and 32-bit AMD Operteron or 64-bit AMD Opteron) Solaris 8 (SPARC only) Solaris 10 Update 9

Table 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	—

Operating System	Available Temporary Disk Space	Other Requirements
HP-UX	582 MB	—
AIX	525 MB	For version 5.x, the Java runtime environment requires these base level file sets or later: <ul style="list-style-type: none"> ■ x11.adt.lib 5.x ■ x11.adt.motif 5.x ■ bos.adt.include 5.x ■ bos.adt.prof 5.x
Solaris	540 MB	—

NOTE The minimum RAM requirement is 512 MB.

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:
 - a. Manually open the `install` folder.
 - b. 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 Sun Customer Care Center 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 Sun Customer Care Center representative if you need to change the installation options.

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`.

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

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

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.

NOTE 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 [Things to Know – In-Band and Out-of-Band Requirements](#).)

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.

Support Monitor Profiler – This package gathers, records, and communicates data about the operation of a storage array. The application is installed with the SANtricity ES Storage Manager if you choose either a Typical or Management Station Installation.

NOTE 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.

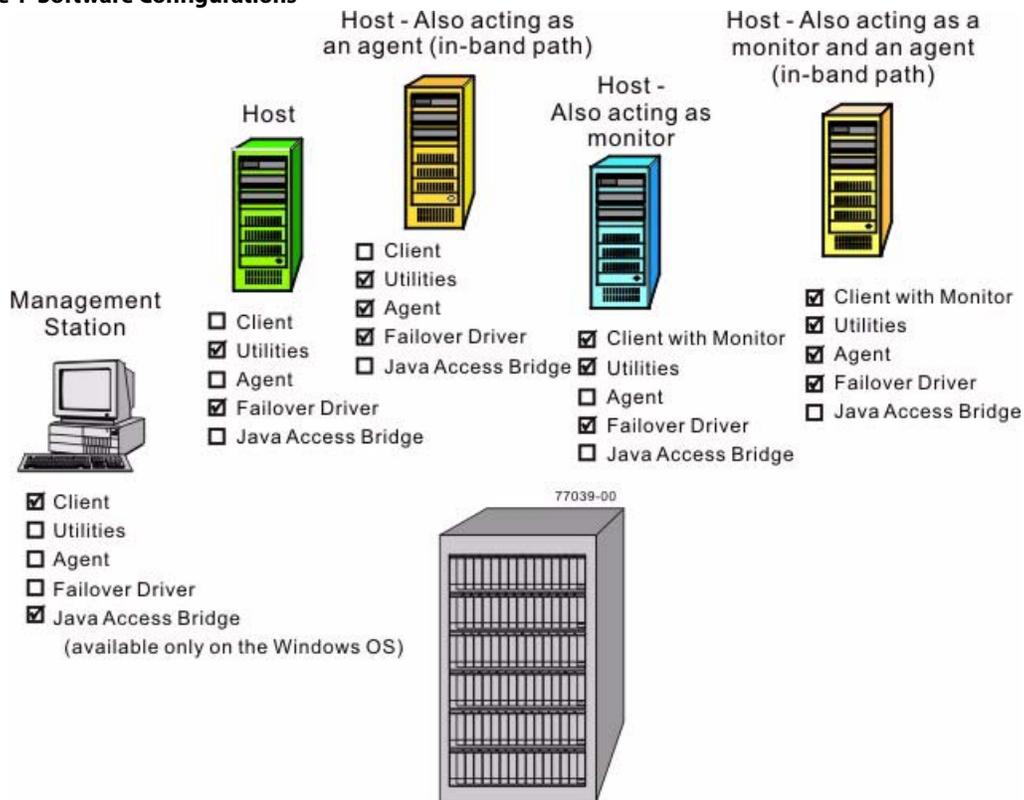
NOTE Use the figures and tables that follow to determine the software packages that should be installed on each machine.

NOTE You must install the utilities and the failover driver on each host that is attached to the storage array.

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

NOTE 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 1 Software Configurations



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

Table 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.

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 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

Java Access Bridge – Enables Windows OS-based assistive technology to access and interact with the application.

Table 5 Software Packages That Are Supported on Each Operating System

Operating System	Client	Utilities	Agent	Failover	JAB
Windows XP and Windows Vista	X	—	—	—	X
Windows Server 2003 and Windows Server 2008	X	X	X	X	X
Red Hat 5.5 Client and SUSE Linux Enterprise Desktop 11.1	X	—	—	—	—
Red Hat Enterprise Linux and SUSE Linux Enterprise Server	X	X	X	Manual ^A	—
Solaris	X	X	X	X	—
HP-UX	X ^B	X	X	X	—
AIX	X	X	X	—	—
NetWare	X ^B	X	X	X	X

^A See [Procedure – Manually Installing RDAC on the Linux OS](#).

^B Windows Client or Linux Client only.

Procedure – Manually Installing RDAC on the Linux OS

1. 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.

2. To clean the directory, type this command, and press Enter:

```
make clean
```
3. To compile the modules, type this command, and press Enter:

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

```
make install
```
5. 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.
6. Read the `Readme.txt` file in the `linuxrdac` directory to complete the RDAC installation process.
7. Reboot or start your host.

Step 4 – Configuring the Host Bus Adapters

Procedure – Configuring the HBAs

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, iSCSI or SAS connections.

This section provides information about configuring HBA settings for your Fibre Channel (FC) connections. For information about configuring HBA settings for iSCSI and SAS connections, refer to the latest *Product Release Notes for SANtricity ES Storage Manager*.

For the latest compatibility information about recommended HBA settings for FC, iSCSI, and SAS connections, refer to the Storage Systems Compatibility Matrix, available at:

<http://www.lsi.com/compatibilitymatrix/>

Use the following table to determine whether you need to make any configuration changes for your HBA that uses a Fibre Channel connection.

Table 6 Configuration Changes for HBAs

HBA Vendor	Configuration Changes Required?	Next Step
Emulex	Yes	<p>Linux OS:</p> <ul style="list-style-type: none"> Procedure – Changing the Emulex HBA Driver Configuration (Linux OS) <p>Solaris OS:</p> <ul style="list-style-type: none"> Procedure – Changing the Emulex HBA Driver Configuration (Solaris OS) <p>Windows Server 2003 OS and Windows Server 2008 OS:</p> <ul style="list-style-type: none"> Procedure – Changing the Emulex HBA Driver Configuration (Windows Server 2003 OS and Windows Server 2008 OS)
Hewlett-Packard (HP)	<p>Yes</p> <ul style="list-style-type: none"> The <i>only</i> factory default setting that you must change is the I/O timeout value. Set the value to 120. You must change the I/O timeout value for each block device (volume) that you create on the storage array. <ul style="list-style-type: none"> Because you must first create the volumes, use the instructions for changing the I/O timeout value in Step 17 – Configuring the Storage 	Step 5 – Starting SANtricity ES Storage Manager
IBM	No	Turning on the Power and Checking for Problems.

HBA Vendor	Configuration Changes Required?	Next Step
LSI	No	"Turning on the Power and Checking for Problems."
QLogic	Yes NOTE – The 2312 model is not a QLogic HBA model. It is a chip on the 2342 model.	Linux OS: <ul style="list-style-type: none"> ■ Procedure – Changing the QLogic HBA Configuration (BIOS Settings) Solaris OS: <ul style="list-style-type: none"> ■ Procedure – Changing the QLogic HBA Configuration (Solaris OS) Windows Server 2003 OS and Windows Server 2008 OS: <ul style="list-style-type: none"> ■ Procedure – Changing the QLogic HBA Configuration (Windows Server 2003 OS and Windows Server 2008 OS) ■ BIOS Settings for QLogic HBAs
Sun	No	Turning on the Power and Checking for Problems.

Procedure – Changing the Emulex HBA Driver Configuration (Linux OS)

NOTE This procedure applies to only the SUSE Linux Enterprise Server 9 OS.

1. Use Emulex's HBAnyware tool to change this value:
`lpfc_nODEV_tmo = 60`
2. Reboot your host.
3. Go to Turning on the Power and Checking for Problems topic at the end of your hardware configuration document.

Procedure – Changing the Emulex HBA Driver Configuration (Solaris OS)

1. Change these values in the `/kernel/drv/lpfc.conf` configuration file:
 - `Automap = value`

Table 7 Supported Values for Automap

Value	Type of Binding
0	Scan persistent binding only
1	World-Wide Node Name (WWNN) binding
2	WWPN binding
3	DID binding

- `No-device-delay = 0`
 - `Network-on = 0`
 - `Linkdown-tmo = 60`
 - `Nodev-tmo = 60`
2. Reboot your host.
 3. Go to Turning on the Power and Checking for Problems at the end of your hardware configuration document.

Procedure – Changing the Emulex HBA Driver Configuration (Windows Server 2003 OS and Windows Server 2008 OS)

ATTENTION Possible data corruption – The Registry Editor is an advanced tool for changing settings. If you make an error in the registry, your computer might not function correctly. Make sure that you back up (export) your registry before you start this task. Refer to the online help topics on your host operating system for more information.

1. Select **Start >> Run** on your operating system.
2. To start the Registry Editor, type `regedit`, and click **OK**.
3. Use the information in the following table to change the various registry values. Double-click the value to change it.

Table 8 Registry Value Changes for Emulex HBAs (Windows Server 2003 OS and Windows Server 2008 OS)

Registry Values	Windows Server 2003 OS and Windows Server 2008 OS
HKEY_LOCAL_MACHINE >> System >> CurrentControlSet >> Services >> elxstor >> Parameters >> Device (under the DriverParameter variable)	
NOTE – DriverParameter is of the type REG_SZ. Add these parameters to the DriverParameter string. Do <i>not</i> create a separate key for each of the parameters.	
LinkTimeOut	60
NodeTimeOut	60
HKEY_LOCAL_MACHINE >> System >> CurrentControlSet >> Services >> md3dsm or mppdsm >> Parameters	
SynchTimeOut (REG_DWORD)	x78
DisableLunRebalance [value_for_cluster] (REG_DWORD)	0x03
NOTE – Change this value only if you are using the Microsoft Cluster Service.	
HKEY_LOCAL_MACHINE >> System >> CurrentControlSet >> Services >> Disk	
TimeOutValue (REG_DWORD)	x78

4. After you change the registry values, reboot your host.
5. Go to Turning on the Power and Checking for Problems at the end of your particular hardware configuration document.

Procedure – Changing the QLogic HBA Configuration (BIOS Settings)

NOTE You need to perform this procedure only if your operating system is the Linux OS, the Windows Server 2003 OS, or the Windows Server 2008 OS. If your operating system is the Solaris OS, go to [Procedure – Changing the QLogic HBA Configuration \(Solaris OS\)](#).

NOTE Instead of using the BIOS utility, you can use the software utility that is supplied with the QLogic HBA.

1. Reboot or start your host.
2. While the host is booting, watch for the prompt, and press Alt-Q to access the BIOS utility.
3. Select an HBA to view its settings.
4. Select **Configuration Settings**, and make the applicable changes using the information in the following table.

Table 9 BIOS Settings for QLogic HBAs

Setting	Linux OS	Windows Server 2003 OS and Windows Server 2008 OS
Host Adapter Settings		
LoopResetDelay	8	
AdapterHardLoopID (recommended only for arbitrated loop topology)	Enabled	
HardLoopID (recommended only for arbitrated loop topology)	Any unique number. Typically set to 20, 21, or 22.	
Advance Adapter Settings		
ExecutionThrottle	256	
LUNsperTarget	0	0
NOTE – 0 activates maximum LUN support.		
EnableTargetReset	Yes	
LoginRetryCount	30	
PortDownRetryCount	35	
LinkDownTimeout	60	

5. Save the changes.
6. Repeat step 3 through step 5 for each QLogic HBA in each host.
7. Reboot your host.
8. Depending on your operating system, go to one of these steps:
 - **Linux OS** – Turning on the Power and Checking for Problems at the end of your particular hardware configuration guide.
 - **Windows Server 2003 OS and Windows Server 2008 OS** – [Procedure – Changing the QLogic HBA Configuration \(Windows Server 2003 OS and Windows Server 2008 OS\)](#).

Procedure – Changing the QLogic HBA Configuration (Solaris OS)

1. Change these values in the `/kernel/drv/qla2300.conf` configuration file:
 - `execution-throttle = 255`
 - `login-retry-count = 30`
 - `enable-adapter-hard-loop-ID = 1` (Recommended only for arbitrated loop topology.)
 - `adapter-hard-loop-ID = 125` (Recommended only for arbitrated loop topology. The ID must be unique for each HBA.)
 - `enable-target-reset = 1`
 - `reset-delay = 8`
 - `port-down-retry-count = 70`
 - `maximum-luns-per-target = 0` (0 activates maximum LUN support.)
2. Reboot your host.
3. Go to “Turning on the Power and Checking for Problems” at the end of your particular hardware configuration guide.

Procedure – Changing the QLogic HBA Configuration (Windows Server 2003 OS and Windows Server 2008 OS)

ATTENTION Possible data corruption – The Registry Editor is an advanced tool for changing settings. If you make an error in the registry, your computer might not function correctly. Make sure that you back up (export) your registry before you start this task. Refer to the online help topics on your host operating system for more information.

1. Select **Start >> Run** on your operating system.
2. To start the Registry Editor, type `regedit`, and click **OK**.
3. Use the information in the following table to change the various registry values. Double-click the value to change it.

Table 10 Registry Value Changes for QLogic HBAs (Windows Server 2003 OS and Windows Server 2008 OS)

Setting	Windows Server 2003 OS and Windows Server 2008 OS
HKEY_LOCAL_MACHINE >> System >> CurrentControlSet >> Services >> QL2300 >> Parameters >> Device	
MaximumSGList (REG_WORD)	0xff
HKEY_LOCAL_MACHINE >> System >> CurrentControlSet >> Services >> QL2300 >> Parameters >> Device under the DriverParameter variable	
NOTE DriverParameter is of type REG_SZ. Add these parameters to the DriverParameter string. Do not create a separate key for each of the parameters.	
BusChange	0
HKEY_LOCAL_MACHINE >> System >> CurrentControlSet >> Services >> Disk	
TimeOutValue (REG_DWORD)	x78
HKEY_LOCAL_MACHINE >> System >> CurrentControlSet >> Services >> md3dsm or mppdsm >> Parameters	
SynchTimeOut (REG_DWORD)	x78
DisableLunRebalance [value_for_cluster] (REG_DWORD)	0x03
NOTE This setting applies only to a cluster configuration.	

4. After you change the registry values, reboot your host.
5. Go to Turning on the Power and Checking for Problems at the end of your particular hardware configuration guide.

Step 5 – Starting SANtricity ES Storage Manager

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 10.77* electronic document topics or to the PDF on the SANtricity ES Storage Manager Installation DVD.
- Online help topics in the Enterprise Management Window and the Array Management Window in SANtricity ES Storage Manager.

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 [Step 6 – Adding the Storage Array](#).

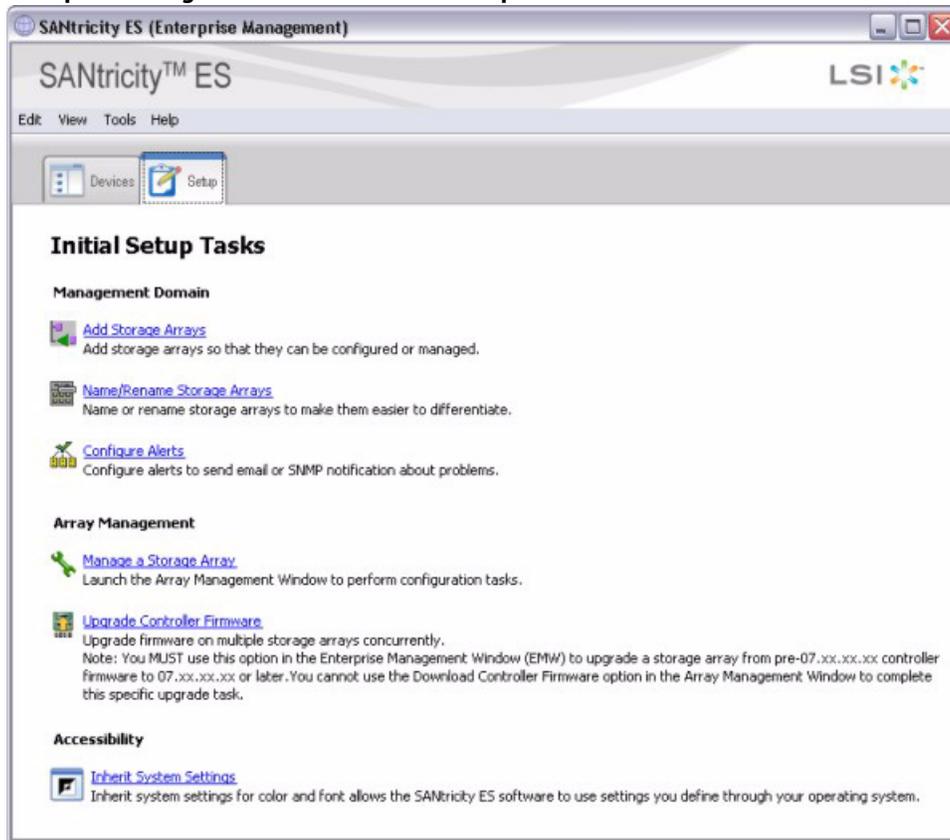
NOTE The Enterprise Management Window and the Array Management Window are the two main windows that you use to manage your storage array. The title at the top of each window identifies its type.

Things to Know – Enterprise Management Window and Array Management Window

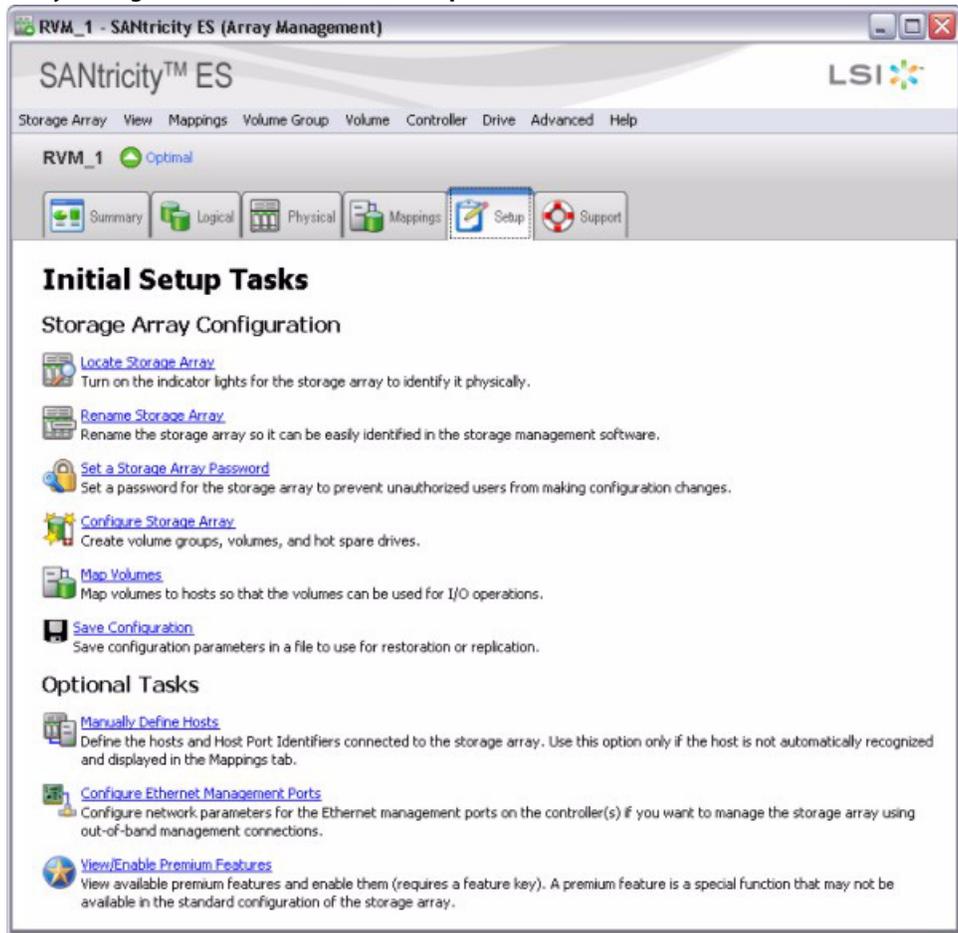
Table 11 Overview of the Enterprise Management Window and the Array Management Window

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>
Array Management Window	<p>It provides you with all of the functions to configure, maintain, and troubleshoot an individual storage array.</p> <p>You launch the Array Management Window from the Enterprise Management Window to manage an individual storage array.</p> <p>Multiple Array Management Windows can appear at the same time (one for each storage array you want to manage).</p>
Enterprise Management Window Setup Tab and Array Management Window Setup Tab	<p>When you first start either the Enterprise Management Window or the Array Management Window, a Setup tab is selected by default.</p> <p>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.</p>

Figure 2 Enterprise Management Window with the Setup Tab Selected



B2005-01

Figure 3 Array Management Window with the Setup Tab Selected

Step 6 – Adding the Storage Array

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 modules first, and then the array module).
- Make sure that you have installed the applicable storage management software.

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 automatically 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 [Step 7 – Naming the Storage Array](#).
 - **No** – Go to [Procedure – Automatically Adding a Storage Array](#) (the storage array might reside outside the local sub-network).

NOTE After adding the storage array, you can view or change the cache memory settings of the storage array. See [Step 14 – Changing the Cache Memory Settings](#).

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 4 Add New Storage Array – Manual Dialog

Add New Storage Array - Manual

LSI

[What are in-band and out-of-band management connections?](#)

[Adding controllers with more than one Ethernet port](#)

[What if my system only has one controller?](#)

Select a management method:

Out-of-band management:
Manage the storage array using the controller Ethernet connections.

Controller (DNS/Network name, IPv4 address, or IPv6 address):

Controller (DNS/Network name, IPv4 address, or IPv6 address):

In-band management:
Manage the storage array through an attached host.

Host (DNS/Network name, IPv4 address, or IPv6 address):

Add Cancel Help

82004-03

2. If you are using the in-band management method, 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.

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

NOTE After adding the storage array, you can view or change the cache memory settings of the storage array. See [Step 14 – Changing the Cache Memory Settings](#).

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.

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

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.

NOTE 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.

Step 7 – Naming the Storage Array

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."

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. In the Warning dialog, 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.

Step 8 – Resolving Problems

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

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 [Step 9 – Adding Controller Information for the Partially Managed Storage Array](#).
 - **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.

Things to Know – Support Monitor Profiler

The Support Monitor Profiler is a software application that gathers, records, and communicates data about the operations of a storage array. The application is installed with the SANtricity ES Storage Manager if you choose a Typical or a Management Station installation. You also can install the Support Monitor Profiler by choosing it as a component during a Custom installation of SANtricity ES Storage Manager.

When the Support Monitor Profiler is installed, the **Profiler Console** icon appears on your desktop. Click the icon to open the application. The Support Monitor Profile allows you to perform the following tasks:

- Register the Support Monitor.
- Scan devices, log and view support data, System-on-a-chip (SOC) and Record-Level Sharing (RLS) change log files, and email support data to the Sun Customer Care Center representative.
- Upgrade to the Full Profiler Support Monitor.

For more information about using the Support Monitor Profiler, refer to the *Support Monitor Installation and Overview* electronic document topics or to the PDF on the SANtricity ES Storage Manager Installation DVD.

Procedure – 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.

NOTE Use this option only under the guidance of your Sun Customer Care Center 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 Sun Customer Care Center 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**.

Step 9 – Adding Controller Information for the Partially Managed Storage Array

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

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.

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.

Procedure– Automatically Adding a Partially-Managed Storage Array

NOTE 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 [Procedure – Rescanning the Host for a New Storage Array](#) to rescan the host.

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.

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

NOTE After adding the storage array, you can view or change the cache memory settings of the storage array. See [Step 14 – Changing the Cache Memory Settings](#).

Step 10 – Manually Configuring the Controllers

Things to Know – Manually Configuring the Controllers

NOTE 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 [Step 1 – Deciding on the Management Method](#) 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 Sun Customer Care Center representative.
- You should configure Ethernet port 2 only if your Sun Customer Care Center 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 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	

NOTE 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 [Procedure – Configuring the Controllers.](#))

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

NOTE 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](#).

NOTE If you connect the management station directly to the Ethernet ports on the array module, 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.

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 FE80:0000:0000:02A0: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](#).

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 5 Change Network Configuration Dialog with IPv4 Settings

Unnamed - Change Network Configuration

LSI

Ethernet port: Controller A, Port 1

Controller A DNS/Network name: em1cfg2a12
Port 1 MAC address: 00:a0:b8:29:e9:84

Speed and duplex mode: 10/100 Mbps, full duplex

Enable IPv4
 Enable IPv6

IPv4 Settings IPv6 Settings

IPv4 Configuration:
 Obtain configuration automatically from DHCP server
 Specify configuration:

IP address:
172 . 22 . 248 . 12

Subnet mask:
255 . 255 . 255 . 0

Controller A gateway:
172.22.248.1
Change Controller Gateway...

OK Cancel Help

76207-03

Figure 6 Change Network Configuration Dialog with IPv6 Settings

The screenshot shows a window titled "Unnamed - Change Network Configuration" with the LSI logo. The "Ethernet port" is set to "Controller A, Port 1". Below it, the "Controller A DNS/Network name" is "em1cfg2a12" and the "Port 1 MAC address" is "00:a0:b8:29:e9:84". The "Speed and duplex mode" is set to "10/100 Mbps, full duplex". There are two checked checkboxes: "Enable IPv4" and "Enable IPv6". The "IPv6 Settings" tab is selected, showing "IPv6 Configuration" with "Specify configuration" selected. The "IP address" field contains "FE80 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000". The "Routable IP address" field contains "0100 : 0000 : 0000 : 0000 : 0200 : 0000 : AEA6 : 2204". The "Controller A router IP Address" field contains "0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000". There is a "Change Controller Router IP..." button. At the bottom are "OK", "Cancel", and "Help" buttons. The version number "78207-04" is in the bottom right corner.

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**.

ATTENTION 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:

- a. Disconnect the Ethernet cable from your management station, and reconnect the Ethernet cables from the controllers into your regular network.
- b. Complete the steps necessary to change the management station's IP address back to what it was originally.

Step 11 – Setting a Password

Things to Know – Passwords

- You need to set a password for your storage array to protect it from serious damage, such as data loss.
- 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.

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

NOTE If you forget your password, you must contact your Sun Customer Care Center representative for help to reset it.

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**.

Step 12 – Removing a Storage Array

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.

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.

NOTE 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.

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

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.

Step 13 – Configuring Email Alerts and SNMP Alerts

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*)

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.

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

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 Sun Customer Care Center 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 Sun Customer Care Center 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.

Step 14 – Changing the Cache Memory Settings

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 module or a storage module is ready to process the data. Cache memory has a faster access time than the actual drive media.

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 module or array module 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.

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.

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 >> Change >> Cache 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**.

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**.

Step 15 – Enabling the Premium Features

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

Key Terms

premium feature

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

Things to Know – Premium Features

You enable a premium feature through a feature key file that you obtain from your storage vendor. The feature key file 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.

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.

Step 16 – 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 [Installing Host Bus Adapters](#) for your particular configuration (ST2500 M2 Array Module, CDE2600-60 array module, 6180 array module, or 6580/6780 controller module) for instructions to obtain these world wide port names.

NOTE If you will not use storage domains or you do not have the Storage Domains premium feature enabled on your storage array, you can skip the information about [Things to Know – Host Groups](#) and [Things to Know – Storage Domains](#), and go to either [Procedure – Defining the Hosts](#) or [Procedure – Defining the iSCSI Hosts](#).

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.

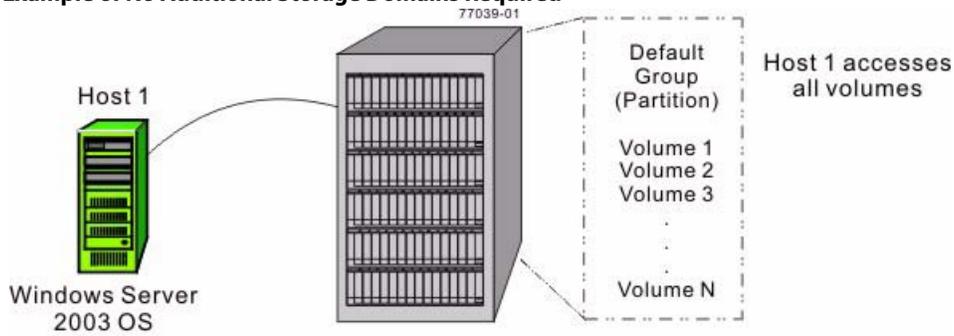
Things to Know – Host Groups

- A host group is a group (cluster) of two or more hosts that share access, in a storage domain, 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 domains.
- If you must define a host group, you can define it through the Define Hosts Wizard described in [Procedure – Defining the Hosts](#).

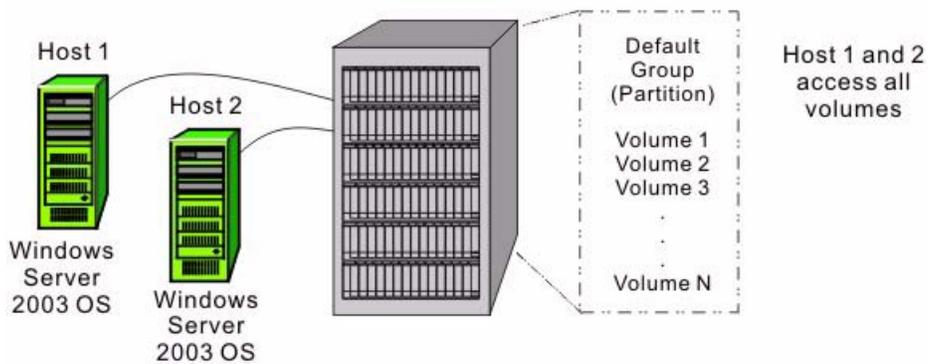
Things to Know – Storage Domains

- A storage domain 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 domain 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.
- Storage Domains 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 domains in this step, but you must understand them to define your hosts.
- You *do not* need to create storage domains if these conditions exist (see the first image below):
 - 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 that 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.
- You *do* need to create storage domains if these conditions exist (see the two images that display with no partition required below):
 - 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 domain for each type of host.

Figure 7 Example of No Additional Storage Domains Required

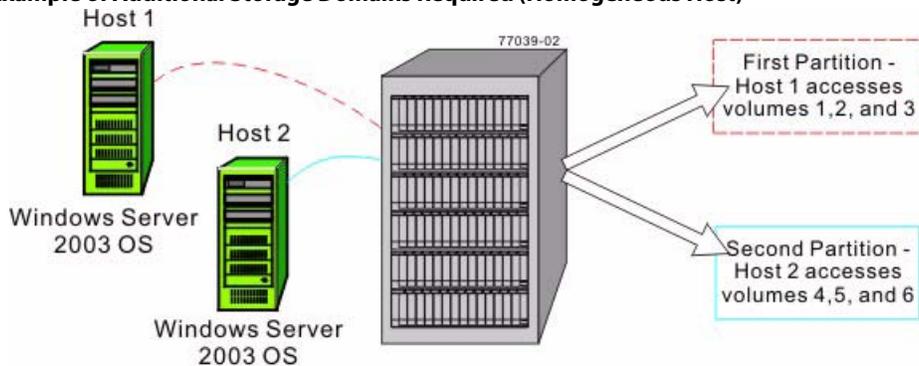


A single host accesses **all** volumes; **no** additional storage partitions are needed.



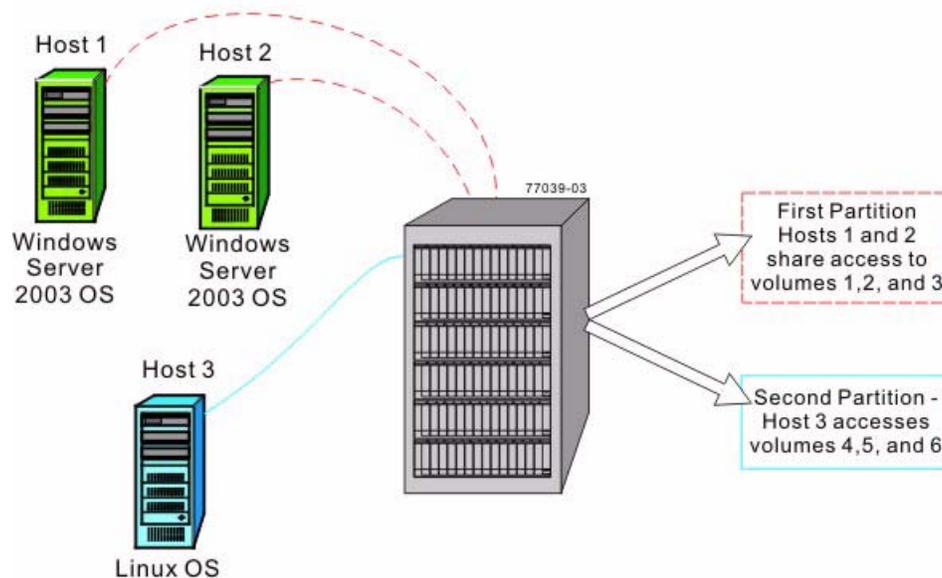
Multiple homogeneous hosts share access to **all** volumes; **no** additional storage partitions are needed and no specific host group is needed.

Figure 8 Example of Additional Storage Domains 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 9 Example of Additional Storage Domains Required (Heterogeneous Hosts)
Host Group 1



- 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.

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.

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.

Step 17 – Configuring the Storage

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 pool 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 Redundant Array of Independent Disks (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 domain

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 pool.

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 pool. Although a volume might consist of more than one drive, a volume appears as one logical component to the host.

pool

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

Things to Know – T10 Protection Information

The T10 Protection Information (PI) premium feature checks for and corrects errors that might occur as data is communicated between a host and a storage array. PI is implemented using the SCSI direct-access block-device protection information model. PI 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 pool that includes DA-capable drives, and then create a volume within that pool 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 pool, select the **Create a T10 Protection Information (PI) 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.

NOTE If a pool is DA-capable and contains a DA-enabled volume, use only DA-capable drives for hot spare coverage. A pool 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 **T10 Protection Information (PI) capable** property is set to **yes**.

Things to Know – Allocating Capacity

- You can create volumes from either unconfigured capacity or free capacity on an existing pool.
 - If you create a volume from unconfigured capacity, you must first specify the parameters for a new pool (RAID level and capacity for a set of drives) before you specify the parameters for the first volume on the new pool.
 - If you create a volume from free capacity, you have to specify the parameters of only the volume, because the pool 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 pools for new capacity requirements
- For hot spare drive protection
- To increase the free capacity on an existing pool 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 pool.
- If you are adding capacity to a T10 Protection Information (PI) -capable pool, use only drives that are PI capable. If you add a drive or drives that are not PI-capable, the pool no longer has PI capabilities, and you no longer have the option to enable PI on newly created volumes within the pool. The PI Capable column in the **Available drives** list shows the PI capabilities of each listed drive.
- If you are adding capacity to a pool that is not DA capable, do not use drives that are DA capable because the pool 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.

Things to Know – Pools and Volumes

- You can create a single volume or multiple volumes per pool. Usually, you will create more than one volume per pool to address different data needs or because of limits on the maximum capacity of a single volume.

NOTE If you choose to copy a T10 Protection Information (PI) enabled source volume to a target volume that is not PI-enabled, you are prompted to confirm your choice. The copy can be completed, but the resulting copy is not PI-enabled. For more information about how volume copy is affected by PI-enabled volumes, refer to *Volume Copy Premium Feature* electronic document topics or the PDF located on the SANtricity ES Storage Manager Installation DVD.

- While creating pools, you must make sure that the drives that comprise the pool are located in different drive modules. This method of creating pools is called module loss protection. Module loss protection guarantees accessibility to the data on the volumes in a pool if a total loss of communication occurs with a single drive module. Communication loss might occur due to loss of power to the drive module or failure of the drive module 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 pool that consists of four or more drives.
 - You can assign RAID Level 1 only to pools with an even number of drives.
 - You can assign RAID Level 3 or RAID Level 5 only to pools with three or more drives.
 - You can assign RAID Level 6 only to pools 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.

Things to Know – Host-to-Volume Mappings and Storage Domains

- 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 domains. 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 domains. Use the Define Storage Domain 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.

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 pools because data redundancy does not exist on these pools.
- A hot spare drive is *not* dedicated to a specific pool 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.

Things to Know – Encryption Services

Drive Security and 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 Drive Security and EKM must be enabled either by you or your storage vendor.

The Drive Security premium feature requires *security-capable* Encryption Services (ES) drives. A security-capable ES 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 pool* from *security-capable* ES drives, the drives in that pool become security enabled. When a *security-capable* ES 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 ES 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 array module, all of the ES 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 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 pool in the storage array from the Pool 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 pool.

Table 13 Pool Security Properties

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

When the 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**

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

NOTE 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 Drive Security premium feature has been enabled, the **Secure Drives** option appears in the **Pool** 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 pool 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 pool is already security enabled.

You can erase security-enabled drives instantly and permanently so that you can reuse the drives in another pool 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 pool, 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 Drive Security premium feature and should not be confused with the pass phrase that is used to protect copies of a Drive Security security key. However, it is good practice to set a storage array password before you create, change, or save a Drive Security security key or unlock secure drives.

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 pools 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 pools, volumes, and hot spare drives. You can choose from a list of suggested configurations, or you can create your own custom configuration.
 - **Create pools and volumes** – This method creates one volume at a time but gives you more control over the pool and volume parameters (such as RAID level, pool, 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 pools, volumes, and hot spare drives, perform one of these actions depending on your storage domain requirements. Refer to the on-screen instructions and the online help topics for more information.
 - **No storage domain is required, and you selected the automatic configuration method** – Go to step 6.
 - **No storage domain 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 domain is required** – Go to step 7.
6. Perform these actions:
 - a. From the **Setup** tab on the Array Management Window, click **Map Volumes**.
 - b. Select the Default Group, and assign each volume a logical unit number (LUN).
 - c. Go to step 8.

NOTE To map all volumes into the Default Group, you should have selected the **Default Mapping** option while creating the volumes.

7. Perform these actions:
 - a. Click the **Mappings** tab.
 - b. Specify the applicable host or host group, volumes, and LUNs.
 - c. Select **Mappings >> Define**, and click **SANshare Storage Partitioning**.
 - d. Refer to the on-screen instructions.
 - e. Repeat step a through step d for each storage domain.
 - f. 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 `cxt.xdx` is the device name of each volume.

```
pvchange -t 120 /dev/dsk/cxt.xdx
```

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 [Procedure – Changing the Cache Memory Settings](#).

Copyright © 2011 LSI Corporation. All rights reserved.
Copyright © 2011 Sun Microsystems, Inc. All rights reserved.
Printed in U.S.A.

