SGI InfiniteStorage 4000 Series and 5000 Series Initial Configuration and Software Installation for SANtricity ES Storage Manager

(ISSM 10.83)

007-5880-001 August 2012

The information in this document supports the SGI InfiniteStorage 4000 series and 5000 series storage systems (ISSM 10.83). Refer to the table below to match your specific SGI InfiniteStorage product with the model numbers used in this document.

SGI Model #	**Netapp Model**	**Netapp Compliance Model**	**Notes**
TP9600H	6091	1500	
TP9700F	6091	1500	
IS4500F	6091	1500	
TP9600F	3994 and 3992	4600	
IS4000H	3994	4600	
IS350	3992	4600	
IS220	1932 1333 DE1300	3600	
IS4100	4900	4600	FC HICs only
IS-DMODULE16-Z	FC4600	4600	
IS-DMODULE60	DE6900	6900	
IS4600	7091	1550	4Gb FC, 8Gb FC, HICs only
IS5012	2600	3650	FC and SAS HICs only
IS5024	2600	5350	
IS5060	2600	6600	
IS-DMODULE12 & IS2212 (JBOD)	DE1600	3650	
IS-DMODULE24 & IS2224 (JBOD)	DE5600	5350	
IS-DMODULE60-SAS	DE6600	6600	
IS5512	5400	3650	
IS5524	5400	5350	
IS5560	5400	6600	

Copyright information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987

Trademark information

NetApp, the NetApp logo, Network Appliance, the Network Appliance logo, Akorri, ApplianceWatch, ASUP, AutoSupport, BalancePoint, BalancePoint Predictor, Bycast, Campaign Express, ComplianceClock, Cryptainer, CryptoShred, Data ONTAP, DataFabric, DataFort, Decru, Decru DataFort, DenseStak, Engenio, Engenio logo, E-Stack, FAServer, FastStak, FilerView, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexSuite, FlexVol, FPolicy, GetSuccessful, gFiler, Go further, faster, Imagine Virtually Anything, Lifetime Key Management, LockVault, Manage ONTAP, MetroCluster, MultiStore, NearStore, NetCache, NOW (NetApp on the Web), Onaro, OnCommand, ONTAPI, OpenKey, PerformanceStak, RAID-DP, ReplicatorX, SANscreen, SANshare, SANtricity, SecureAdmin, SecureShare, Select, Service Builder, Shadow Tape, Simplicity, Simulate ONTAP, SnapCopy, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapManager, SnapMigrator, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapSuite, SnapValidator, SnapVault, StorageGRID, StoreVault, the StoreVault logo, SyncMirror, Tech OnTap, The evolution of storage, Topio, vFiler, VFM, Virtual File Manager, VPolicy, WAFL, Web Filer, and XBB are trademarks or registered trademarks of NetApp, Inc. in the United States, other countries, or both.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at *www.ibm.com/legal/copytrade.shtml.*

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

Table of Contents

Step 1 - Deciding on the Management Method

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

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

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 – 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 “Manually Configuring the Controllers” on page 31 for details.

1. Use the key terms and the following figures to determine the management method that you will use.
2. After reading the information in this section, add a check mark next to the management method that you will use.
   - __ In-band management method
   - __ Out-of-band management method
   - __ In-band management method and out-of-band management method

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

Figure 1 In-Band Management Topology

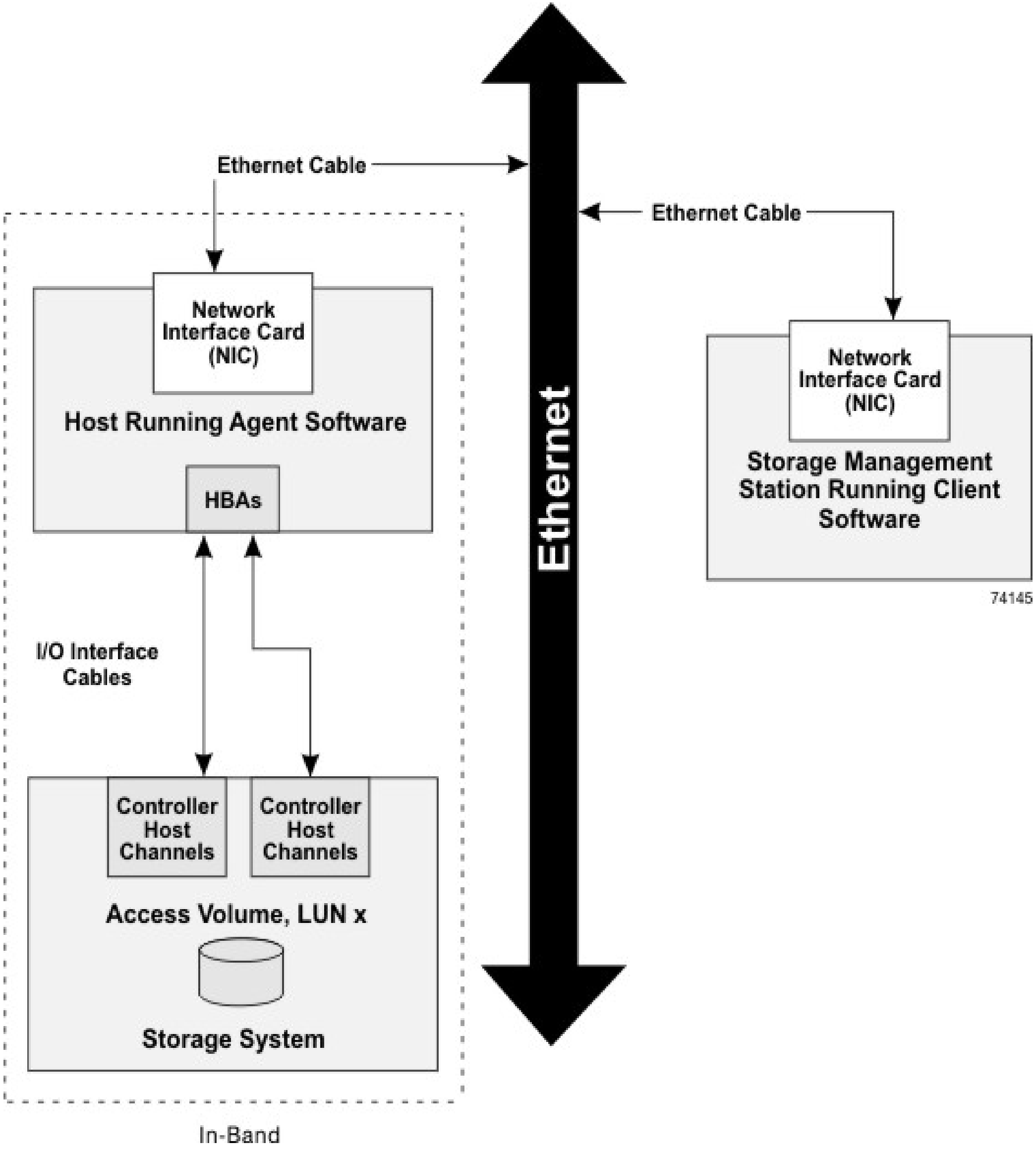
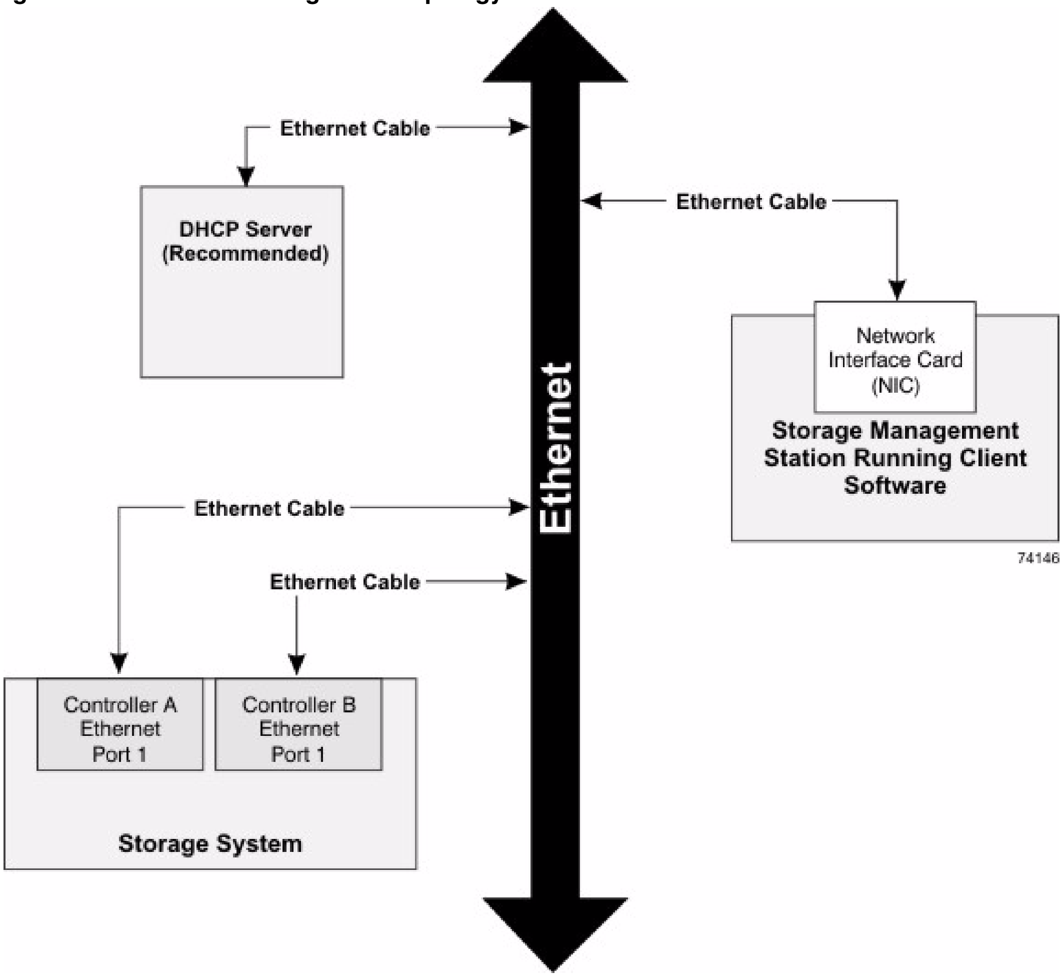


Figure 2 Out-of-Band Management Topology


Ethernet Cable
DHCP Server (Recommended)
Ethernet Cable
Network Interface Card (NIC)
Storage Management Station Running Client Software
Ethernet
Ethernet Cable
Ethernet Cable
74146
Controller A Ethernet Port 1
Controller B Ethernet Port 1
Storage System

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 *without* a DHCP server	Connect separate Ethernet cables to each controller. Manually configure the network settings on the controllers. See "Manually Configuring the Controllers" on page 31 for more information.	This method does not use a logical unit number (LUN) on the host. You do not need to install the host-agent software. This method does not use the SAS, Fibre Channel, or iSCSI bandwidth for storage array management functions.	You must manually configure the network settings on the controllers. Ethernet cables are required.

Management Method	Requirements	Advantages	Disadvantages
Out-of-band – IPv6 stateless address auto-configuration *without* a DHCP server (IPv6 networks only)	Connect separate Ethernet cables to each controller. Connect at least one router for sending the IPv6 network address prefix in the form of router advertisements. The router is necessary to route the IPv6 packets outside the local network.	No additional manual network configuration is required on the controllers. By default, the controllers automatically obtain their IP addresses by combining the auto-generated link local address and the IPv6 network address prefix after you turn on the power to the controller-drive tray. You do not need to install host-agent software. This method does not use a LUN on the host. This method does not use the SAS, Fibre Channel or iSCSI bandwidth for storage array management functions.	Ethernet cables are required.
Out-of-band *with* a DHCP server (IPv4 networks only)	Connect separate Ethernet cables to each controller. Assign either static IP addresses or dynamic IP addresses to the controllers. It is recommended that you assign static IP addresses. Check your DHCP server for the IP addresses that are associated with the media access control (MAC) addresses of the controllers. The MAC address appears on a label on each controller in the form: *xx.xx.xx.xx.xx.xx*. 00.A0.B8.00.00.00 00.A0.B8.00.00.00 1T12345678 1T12345678	No additional manual network configuration is required on the controllers. By default, the controllers automatically obtain their IP addresses from the DHCP server after you turn on the power to the controller-drive tray. You do not need to install host-agent software. This method does not use a LUN on the host. This method does not use the SAS, Fibre Channel or iSCSI bandwidth for storage array management functions.	Ethernet cables are required.

Management Method	Requirements	Advantages	Disadvantages
In-band	Install host-agent software on at least one of the network-attached hosts. The host-agent software is included with the storage management software. This method requires a special access volume to communicate. This volume is created automatically.	No additional manual network configuration is required on the controller.	This method uses both a LUN on the host and the SAS, Fibre Channel or iSCSI bandwidth for storage array management functions.

Step 2 - 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 Setting Up the Storage Array for Windows Server 2008 Server Core on page 4. If you are not running Windows Server 2008 Server Core, start with the tasks in this step.

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 Fibre Channel or SAS HBA host ports, or the iSCSI NIC host ports and the corresponding 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.

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.

Some operating systems support using the storage array as a boot device. For assistance with setting up this configuration, refer to your storage vendor for compatibility information and your HBA vendor for specific SAN boot instructions.

Things to Know – Specific Operating Systems

NOTE For more information about each operating system, refer to "Things to Know – System Requirements" on page 9.

HP-UX 11.31 (IA64 and PA-RISC):

- This operating system provides full client, agent, and util support of the SANtricity ES Storage Manager.
- Supports both in-band and out-of-band management.

Red Hat Enterprise Linux Desktop 5 Client OS, Red Hat Enterprise Linux Desktop 6 Client OS, SUSE Desktop 10 OS, and SUSE Desktop 11 OS:

- These operating systems support only the SANtricity ES Storage Manager Client package.
- Systems running these operating systems can be used only as storage management stations.

Red Hat Enterprise Linux Server 5.7 OS, Red Hat Enterprise Linux Server 6.1 OS, SUSE Linux Enterprise Server 10.4 OS, and SUSE Linux Enterprise Server 11.1 OS:

- These operating systems provide full client, agent, and util support of the SANtricity ES Storage Manager.
- Supports both in-band and out-of-band management.
- These operating systems support the use of the SteelEye® LifeKeeper and Native Red Hat Clustering software for node failover. Linux Infiniband uses Lustre for node failover.
- The Linux Red Hat 6.1 Client OS also supports the native device mapper application.

Solaris 10 u9 OS and Solaris 11OS:

- These operating systems provide full client, agent, and util support of the SANtricity ES Storage Manager.
- Supports both in-band and out-of-band management.
- The Solaris OS supports the use of the Multiplexed I/O (MPxIO) driver.
- The Solaris OS supports the use of the Sun Cluster software for clustering.

VMware 4.1u2 OS and VMware 5.0 OS:

- These operating systems provide no client, agent, or util support of the SANtricity ES Storage Manager.
- Supports out-of-band management only from another support operating system.

Windows XP OS and Windows Server 2003 latest Web Edition OS:

- These operating systems support the SANtricity ES Storage Manager Client package only.
- Systems running these operating systems can be used only as storage management stations with no I/O attach. Both 32-bit and 64-bit modes are supported.

Windows Server 2008 R2 SP1 (standalone) Windows Server 2008 OS R2 SP1:

- These operating systems support the use of the Microsoft Multi-Path I/O (MPIO) driver for failover using the NetApp DSM.
- These operating systems support the use of the Microsoft Cluster Server for node failover.

Things to Know – System Requirements

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

Table 2 Operating System Version or Edition Requirements

Operating System	System and Version or Edition
HP-UX	**OS Versions for I/O attach hosts**: HP-UX 11.31 March 2011 (IA64 and PA-RISC Full Client, Agent, and util support is available, as well as both in-band and out-of-band management . **Processors supported**: ■ Itanium 2 ■ PA-RISC **JRE level:** 1.6.x **I/O Path Fail-over**: Target Port Group Support (TPGS) with Asymmetric Logical Unit Access (ALUA) support
Linux	**OS Versions for I/O attach hosts**: ■ Linux Red Hat 5.7 ■ Linux Red Hat 6.1 ■ SUSE Linux Enterprise Server 10.4 ■ SUSE Linux Enterprise Server 11.1 Full Client, Agent, and util support is available, as well as both in-band and out-of-band management. **OS Versions for the GUI client only (no I/O attach):** ■ Linux Red Hat 5 Client ■ Linux Red Hat 6 Client ■ SUSE Linux Enterprise Server 10 Client ■ SUSE Linux Enterprise Server 11 Client All support 32-bit only so the client can be used as a Management Station. **Processors supported**: ■ Intel Xeon 32-bit and 64-bit ■ AMD Opteron 32-bit and 64-bit **JRE level:** 1.6.x **I/O Path Fail-over**: DM-MP Depending on your operating system release level, additional steps might be required to enable DM-MP with ALUA support. If SANtricity ES shipped with the DVD, the patches are on the DVD. If SANtricity ES did not ship with the DVD, refer to your storage vendor’s website to download the patches.

Operating System	System and Version or Edition
Linux (Infiniband)	**OS Versions for I/O attach hosts**: ■ Linux Red Hat 6.1 ■ Linux Red Hat 5.6 Only Client support with out-of-band management support is available. **OS Versions for the GUI client only (no I/O attach):** ■ Linux Red Hat 5 Client ■ Linux Red Hat 6 Client ■ SUSE Linux Enterprise Server 10 Client ■ SUSE Linux Enterprise Server 11 Client All support 32-bit only so that the client can be used as a management station. **Processors supported**: ■ Intel Xeon 32-bit and 64-bit ■ AMD Opteron 32-bit and 64-bit **JRE level:** 1.6.x **I/O Path Fail-over**: DM-MP Depending on your operating system release level, additional steps may be required to enable DM-MP support. If SANtricity ES shipped with the DVD, the patches are on the DVD. If SANtricity ES did not ship on the DVD, refer to your storage vendor's website to download the patches.
Macintosh OS X	**OS Versions for I/O attach hosts**: ■ Macintosh 10.6 ■ Macintosh 10.7 No Client, Agent, or Util support, and only out-of-band management is supported through another supported operating system or guest operating system. **OS Versions for I/O attach only** **I/O Path Fail-over**: Uses Target Port Group Support (TPGS)
Solaris SPARC-based system (FC only)	**OS Versions for I/O attach hosts**: ■ Solaris 10 u9 ■ Solaris 11 Full Client, Agent, and util support is available, as well as both in-band and out-of-band management. **Processors supported**: Sun Sparc **JRE level:** 1.6.x **I/O Path Fail-over**: MPxIO on Solaris 10 and on Solaris 11. Note that ALUA is supported only in Solaris 11.

Operating System	System and Version or Edition
Solaris x86 (FC only)	**OS Versions for I/O attach hosts**: ■ Solaris 10 u9 ■ Soaris 11 Full Client, Agent, and util support is available, as well as both in-band and out-of-band management. **Processors supported**: ■ Intel Xeon 32-bit and 64-bit ■ AMD Opteron 32-bit and 64-bit **JRE level:** 1.6.x **I/O Path Fail-over**: MPxIO on Solaris 10 and on Solaris 11. Note that ALUA is supported only in Solaris 11.
VMware	**OS Versions for I/O attach hosts**: ■ 4.1u2 ■ 5.0 (M/N release) No Client, Agent, or Util support, and only out-of-band management is supported through another supported operating system or guest operating system. **OS Versions for the GUI client only (no I/O attach):** None.: the Management client must be run on another OS. **Processors supported**: ■ Intel Xeon 64-bit ■ AMD Opteron 64-bit **I/O Path Fail-over**: VMware native failover using Target Port Group Support (TPGS) with ALUA support
Windows Server 2003 SP2 R2	**OS Versions for I/O attach hosts**: ■ Standard Edition ■ Enterprise Edition ■ Datacenter Edition **OS Versions for the GUI client only (no I/O attach):** ■ XP Professional SP3 ■ The latest Web Edition **Processors supported**: ■ Intel Xeon 32-bit and 64-bit ■ AMD Opteron 32-bit and 64-bit **JRE level:** 1.6.x **I/O Path Fail-over**: Microsoft MPIO using the NETApp DSM

Operating System	System and Version or Edition
Windows Server 2008 R2 SP1 (64-bit only)	**OS Versions for I/O attach hosts**: ■ Standard Server and Core ■ Enterprise Server and Core ■ Datacenter Server and Core ■ Foundation Server and Core **Hypervisor OS Version for I/O attach:** ■ Hyper-V Server 2008 R2 SP1 (standalone) for client-only support (out-of-band management method only supported) ■ Windows Server 2008 RE2 SP1 Hyper-V (an add-on to Windows Server 2008) **OS Versions for the GUI client only (no I/O attach):** ■ Windows Vista SP1 ■ Windows 7 ■ Windows XP **Processors supported**: ■ Intel Xeon 64-bit ■ AMD Opteron 64-bit **JRE level:** 1.6.x **I/O Path Fail-over**: Microsoft MPIO using the NETApp DSM

Table 3 Temporary Disk Space Requirements

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

NOTE The minimum RAM requirement is 512 MB.

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 Technical Support representative if you need to change the installation options.

   — When using the `silent` parameter during the installation, the command installs the storage management software using all of the defaults. A silent installation uses a resource file that contains all of the required information, and it does not return any windows until the installation is complete. This installation does not use a GUI. Contact your Technical Support 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" on page 4).

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.

Consult the *Failover Drivers Guide* to see if your operating system requires a multi-path driver upgrade.

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

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.

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

NOTE If you choose not to automatically enable the event monitor during installation, you do 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 3 Software Configurations

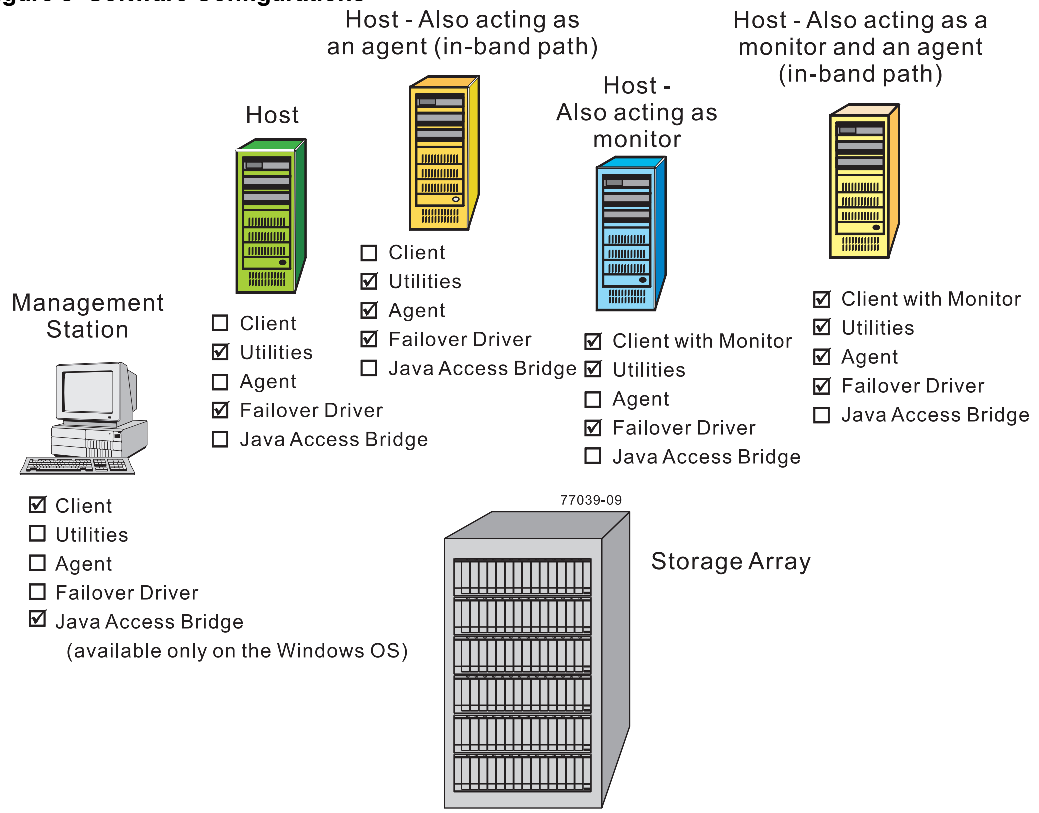


Table 4 Different Machines and Required Software

Machine	Minimum Software Required	Installation Package (Choose One) (See the tables that follow)	Notes
Management station	Client	■ Typical Installation ■ Management Station ■ Custom	■ Click **No** to the prompt, `Automatically start Monitor?` ■ You must choose **Custom** if you want to install the Java Access Bridge software.
Host	■ Utilities ■ Failover driver	■ Typical Installation ■ Host ■ Custom	■ Click **No** to the prompt, `Automatically start Monitor?` ■ Be aware that some operating systems require the manual installation of the RDAC failover driver.
Host – Also acting as an agent for the in-band management method	■ Utilities ■ Agent ■ Failover driver	■ Typical Installation ■ Host ■ Custom	Click **No** to the prompt, `Automatically start Monitor?`

Machine	Minimum Software Required	Installation Package (Choose One) (See the tables that follow)	Notes
Host – Also acting as a monitor for sending critical alerts	■ Client ■ Utilities ■ Failover driver	■ Typical Installation ■ Custom	■ 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	■ Client ■ Utilities ■ Agent ■ Failover driver	■ Typical Installation ■ Custom	■ Click **Yes** to the prompt, `Automatically start Monitor?` ■ Start the monitor on only one host that will run continuously.

Table 5 Installation Wizard Selections

Type of Installation	Client	Utilities	Agent	Failover	JAB[a]
Typical Installation	X	X	X	X	—
Management Station	X	—	—	—	—
Host Station	—	X	X	X	—
Custom (you select the packages)	X	X	X	X	X

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

Table 6 Software Packages That Are Supported on Each Operating System

Operating System	Client	Utilities	Agent	Failover	JAB
Windows Server 2003 and Windows XP	X	X	X	—	X
Windows Server 2008 R2 SP1 (64 bit only), Windows Hyper-V, and Windows Vista	X	X	X	X[a]	X
Windows Vista	X	X	X	—	X
VMware 4.1 u2 and 5.0	—	—[b]	—	X[c]	—
Red Hat 5.7, Red Hat 6.1, Red Hat 6.2, SUSE Linux Enterprise Desktop 10.4, SUSE Linux Enterprise Desktop 11.1, and SUSE Linux Enterprise Desktop 11.2	X	X	X	X[d]	X
Red Hat 6.1 Client and SUSE Linux Enterprise Desktop 11.1 (Infiniband)	X	—	—	X	—
Solaris Sparc (FC only)	X	X	X	X	X
Solaris x86 (FC only)	X	X	X	X	X
Macintosh 10.6 and 10.7	—	—	—	X	—
HP-UX 11.31 (FC only)	X	X	X	X[e]	X

[a] To allow for co-existence with storage arrays running earlier versions of SANtricity ES, the Failover driver can support both Windows RDAC mode (previous versions) and Windows ALUA mode (the current version).

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

[c] Uses VMware native failover driver, using TPGS (Target Port Group Support) with ALUA support. Depending on the OS level, the claim rules may need to be updated to use the **VMW_SATP_ALUA** policy. For specific instructions, please refer to the *Failover Driver Guide*.

[d] For both Red Hat 6.1 and SUSE Linux Enterprise Desktop 11.1, NetApp provides out-of-box DM-MP drivers and Multipath tool binaries for users to install separately.

These patches are required. For specific instructions, please refer to the *Failover Driver Guide*.

For both Red Hat 6.2 and SUSE Linux Enterprise Desktop 11.2, NetApp provides all required changes to support the RDAC handler with ALUA support in the current installation package.

[e] Uses TPGS with ALUA support through the OS.

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 trays into an executable so RDAC can be installed, type this command, and press Enter:

   ```
   make
   ```

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

   ```
   make install
   ```

5. After the make installation 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 3 - Configuring the Host Bus Adapters

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

Please refer to your storage vendor for host operating system, driver, and component compatibility information, as well as any specific configuration requirements or restrictions.

When configuring the failover or multi-path driver, refer to the *Failover Drivers Guide* for detailed information about configuring these drivers. There might be additional steps required to configure the drivers for Asymmetric Logical Unit Access (ALUA) support, which is new with SANtricity Version 10.83. ALUA is a feature of the controllers that provides access to a volume through any controller port.

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

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

- If your host is not running Windows Server 2008 Core, go to "Installing the SANtricity ES Storage Manager Software" on page 7 to continue the installation.
- If your host is running Windows Server 2008 Server Core, you must use the command line and the procedures in this topic to install and configure your storage array.

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

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

Refer to the *Microsoft iSCSI Software Initiator 2.*x *Users Guide* for more information about the commands used in these steps. Refer to the Microsoft Developers Network (MSDN) for more information about Windows Server 2008 Server Core. You can access these resources from `www.microsoft.com`.

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

1. Install the storage management software using "Installing the SANtricity ES Storage Manager Software" on page 7.
2. Configure your storage array using "Configuring the Storage" on page 61.

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 the previous two 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 Technical Support representative if you need to change the installation options.

   When you specify the `silent` parameter during the installation, the command installs the storage management software using all of the defaults. A silent installation uses a resource file that contains all of the required information, and it does not return any windows until the installation is complete. This installation does not use a graphical user interface (GUI). Contact your Technical Support representative if you need to change the installation options.
3. Make sure that the appropriate files are listed in the installation directory (for example, `C:\Program Files\StorageManager`).

   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 the *Command Line Interface and Script Commands for Version 10.83* PDF on the SANtricity ES Storage Manager Installation DVD for instructions on how to configure the iSCSI ports in the "iSCSI Commands" topic. The information in the *Configuring and Maintaining a Storage Array Using the Command Line Interface* 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 also can establish a CHAP user name and password when you configure the target.

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

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

   In this command, <*IP Address Target Controller*> is the IP address for the target port that you are configuring.
3. If you *are* using CHAP, type this command for each port on the target from the command line. When you are finished, go to step 4.

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

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

   ```
   iscsicli ListTargets
   ```

   A list of all found targets appears.

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. Please refer to your storage vendor for host operating system, driver, and component compatibility information, as well as any specific configuration requirements or restrictions that might apply to your storage array, and then make sure that you complete the "Configuring the Storage" on page 61 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 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:

- The *SANtricity ES Storage Manager Concepts for Version 10.83* 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 "Adding the Storage Array" on page 37.

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.

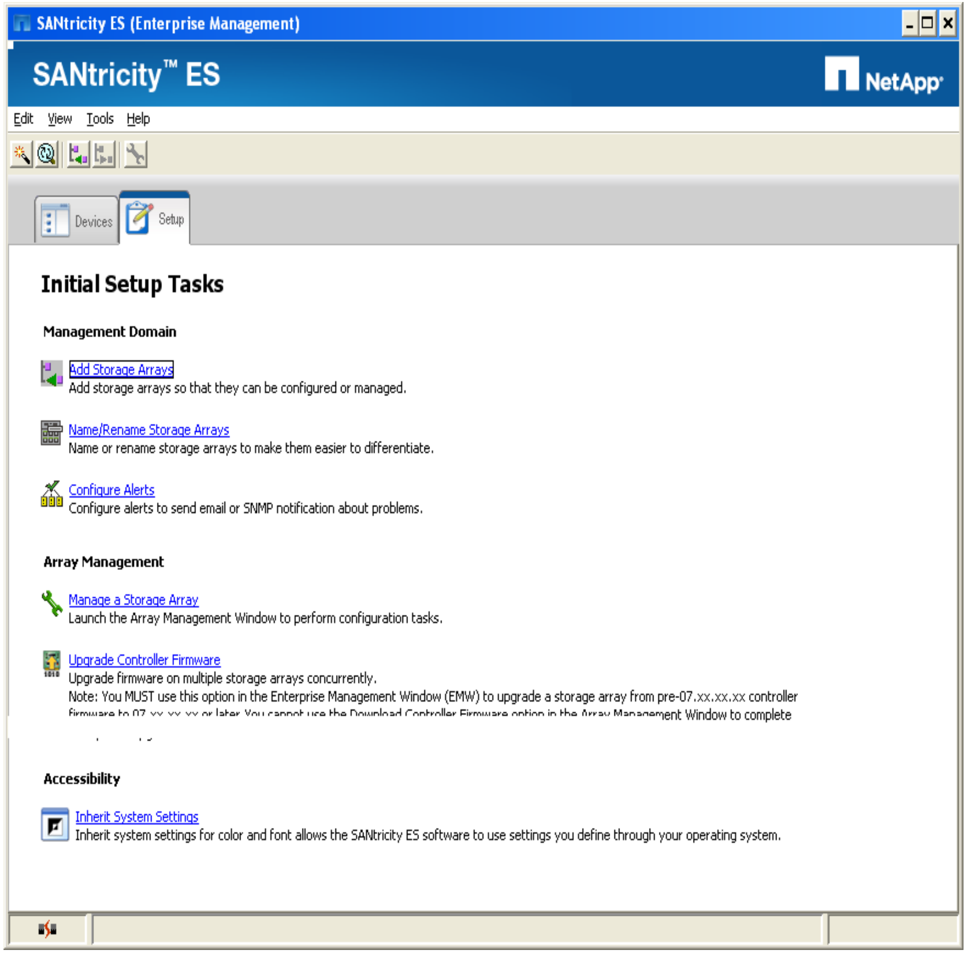
Things to Know – Enterprise Management Window and Array Management Window

Table 7 Overview of the Enterprise Management Window and the Array Management Window

User Interface	Description
Enterprise Management Window	It is the main window that you see when you first start SANtricity ES Storage Manager. It provides you with a view of all of the storage arrays, including the partially managed storage arrays, in your management domain. 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. It provides a high-level status of the health of each storage array. It allows you to manage and configure an individual storage array by launching the Array Management Window.
Array Management Window	It provides you with all of the functions to configure, maintain, and troubleshoot an individual storage array. You launch the Array Management Window from the Enterprise Management Window to manage an individual storage array. Multiple Array Management Windows can appear at the same time (one for each storage array you want to manage).

User Interface	Description
Enterprise Management Window **Setup** Tab and Array Management Window **Setup** Tab	When you first start either the Enterprise Management Window or the Array Management Window, a **Setup** tab is selected by default. The **Setup** tab provides quick access to common setup tasks. The tasks shown are different, depending on the window from which the **Setup** tab was launched.

Figure 4 Enterprise Management Window with the Setup Tab Selected



Initial Setup Tasks

Management Domain

Add Storage Arrays
Add storage arrays so that they can be configured or managed.

Name/Rename Storage Arrays
Name or rename storage arrays to make them easier to differentiate.

Configure Alerts
Configure alerts to send email or SNMP notification about problems.

Array Management

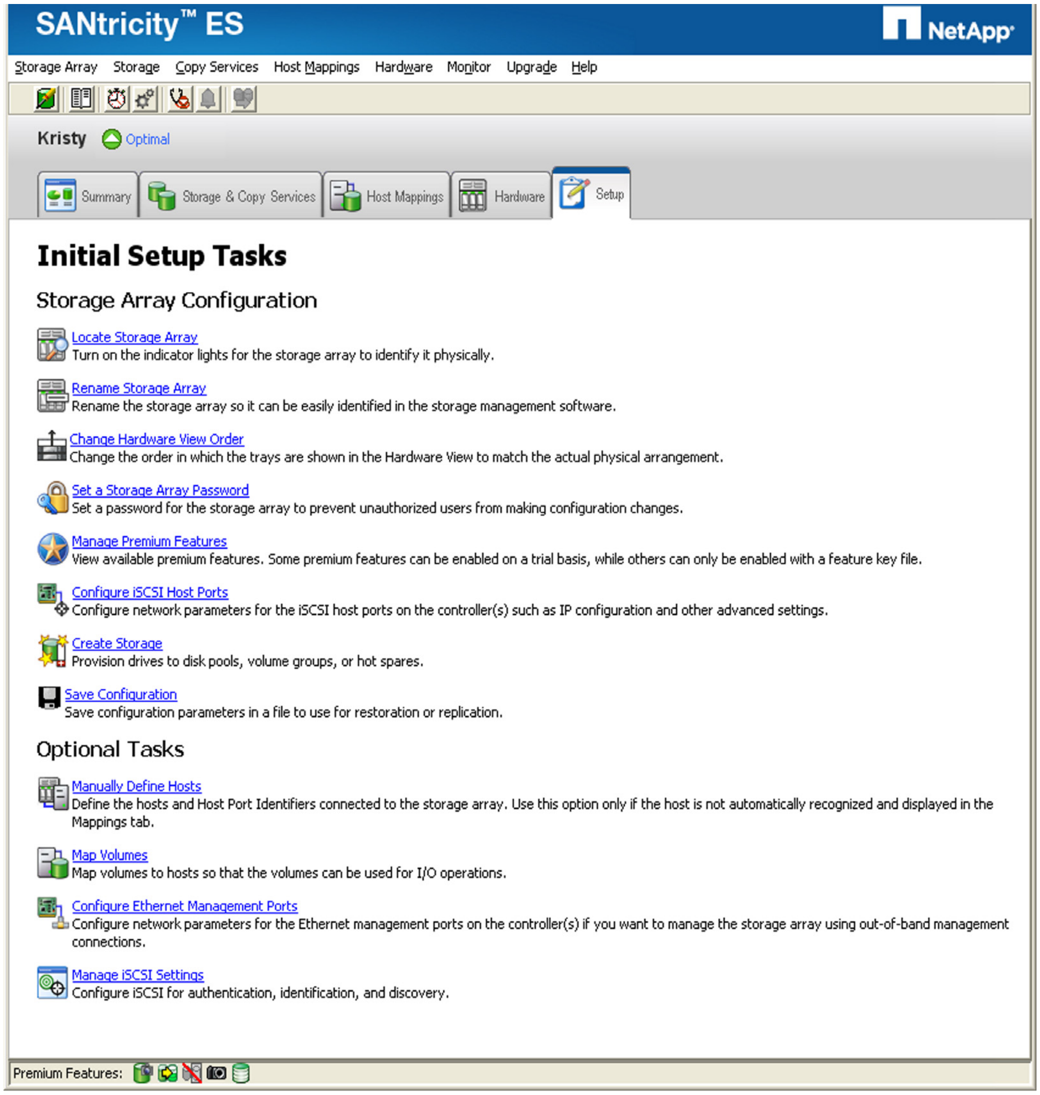
Manage a Storage Array
Launch the Array Management Window to perform configuration tasks.

Upgrade Controller Firmware
Upgrade firmware on multiple storage arrays concurrently.
Note: You MUST use this option in the Enterprise Management Window (EMW) to upgrade a storage array from pre-07.xx.xx.xx controller firmware to 07.xx.xx.xx or later. You cannot use the Download Controller Firmware option in the Array Management Window to complete

Accessibility

Inherit System Settings
Inherit system settings for color and font allows the SANtricity ES software to use settings you define through your operating system.

Figure 5 Array Management Window with the Setup Tab Selected



SANtricity™ ES
NetApp
Storage Array Storage Copy Services Host Mappings Hardware Monitor Upgrade Help
Kristy Optimal
Summary Storage & Copy Services Host Mappings Hardware Setup

Initial Setup Tasks

Storage Array Configuration

Locate Storage Array
Turn on the indicator lights for the storage array to identify it physically.

Rename Storage Array
Rename the storage array so it can be easily identified in the storage management software.

Change Hardware View Order
Change the order in which the trays are shown in the Hardware View to match the actual physical arrangement.

Set a Storage Array Password
Set a password for the storage array to prevent unauthorized users from making configuration changes.

Manage Premium Features
View available premium features. Some premium features can be enabled on a trial basis, while others can only be enabled with a feature key file.

Configure iSCSI Host Ports
Configure network parameters for the iSCSI host ports on the controller(s) such as IP configuration and other advanced settings.

Create Storage
Provision drives to disk pools, volume groups, or hot spares.

Save Configuration
Save configuration parameters in a file to use for restoration or replication.

Optional Tasks

Manually Define Hosts
Define the hosts and Host Port Identifiers connected to the storage array. Use this option only if the host is not automatically recognized and displayed in the Mappings tab.

Map Volumes
Map volumes to hosts so that the volumes can be used for I/O operations.

Configure Ethernet Management Ports
Configure network parameters for the Ethernet management ports on the controller(s) if you want to manage the storage array using out-of-band management connections.

Manage iSCSI Settings
Configure iSCSI for authentication, identification, and discovery.

82005-02

Step 6 - Manually Configuring the Controllers

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

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 "Deciding on the Management Method" on page 1 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 Technical Support representative.
- You should configure Ethernet port 2 only if your Technical Support representative asks you to do so.
- You can configure a gateway on only one of the Ethernet ports on each controller.
- Ethernet port 1 and Ethernet port 2 must be on different sub-networks.
- You can select one of the following speed and duplex mode combinations for your Ethernet ports. If you select the auto-negotiate option, the controller uses the highest speed supported by the Ethernet connection.

Table 8 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" on page 33.)

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" on page 33.

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 controller-drive tray other than a E5400 controller-drive tray, you must use an Ethernet crossover cable. The Ethernet crossover cable is a special cable that reverses the pin contacts between the two ends of the cable.

The E5400 controller-drive trays use Auto-MDIX (automatic medium-dependent interface crossover) technology to detect the cable type and configure the connection to the management station accordingly.

Procedure – Configuring the Management Station

1. Change the IP address on the TCP/IP port on the management station from an automatic assignment to a manual assignment by using the default IP address subnet of the controllers.

   — Make note of the current IP address of the management station so that you can revert back to it after you have completed the procedure.

   — You must set the IP address for the management station to something other than the controller IP addresses (for example, use 192.168.128.100 for an IPv4 network, or use FE80:0000:0000:0000:02A0:B8FF:FE29:1D7C for an IPv6 network).

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

   — If your network is an IPv4 network, check the subnet mask to verify that it is set to 255.255.255.0, which is the default setting.

— Refer to your operating system documentation for instructions about how to change the network settings on the management station and how to verify that the address has changed.

2. After you have configured your management station, perform the procedure in "Procedure – Configuring the Controllers."

Procedure – Configuring the Controllers

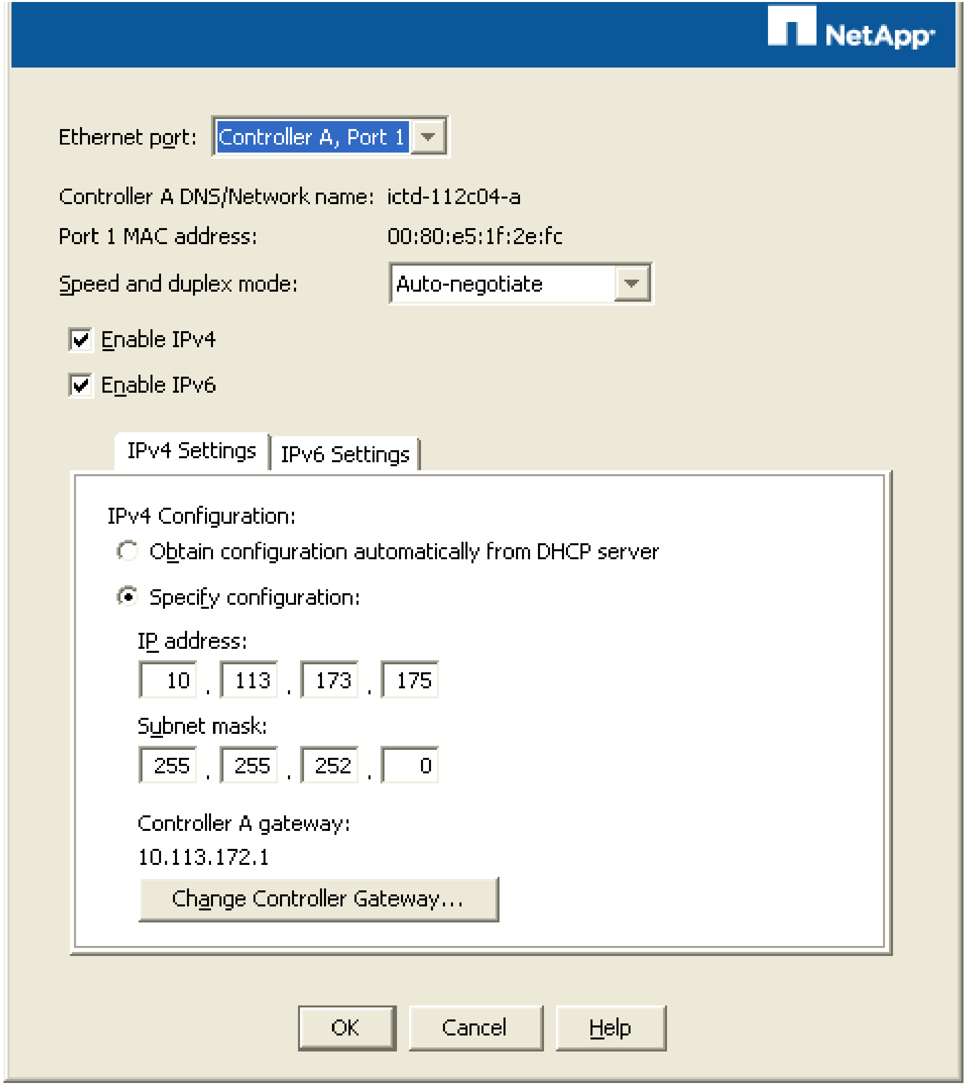
1. In the **Devices** tab on the Enterprise Management Window, double-click the storage array for which you want to configure the controller network settings.

   The associated Array Management Window is launched.

2. Click the **Hardware** tab.

3. Highlight controller A in the Hardware pane of the Array Management Window, and select **Hardware >> Controller >> Configure >> Management Ports**.

Figure 6 Change Network Configuration Dialog with IPv4 Settings



Ethernet port: Controller A, Port 1

Controller A DNS/Network name: ictd-112c04-a

Port 1 MAC address: 00:80:e5:1f:2e:fc

Speed and duplex mode: Auto-negotiate

☑ Enable IPv4

☑ Enable IPv6

IPv4 Settings | IPv6 Settings

IPv4 Configuration:

○ Obtain configuration automatically from DHCP server

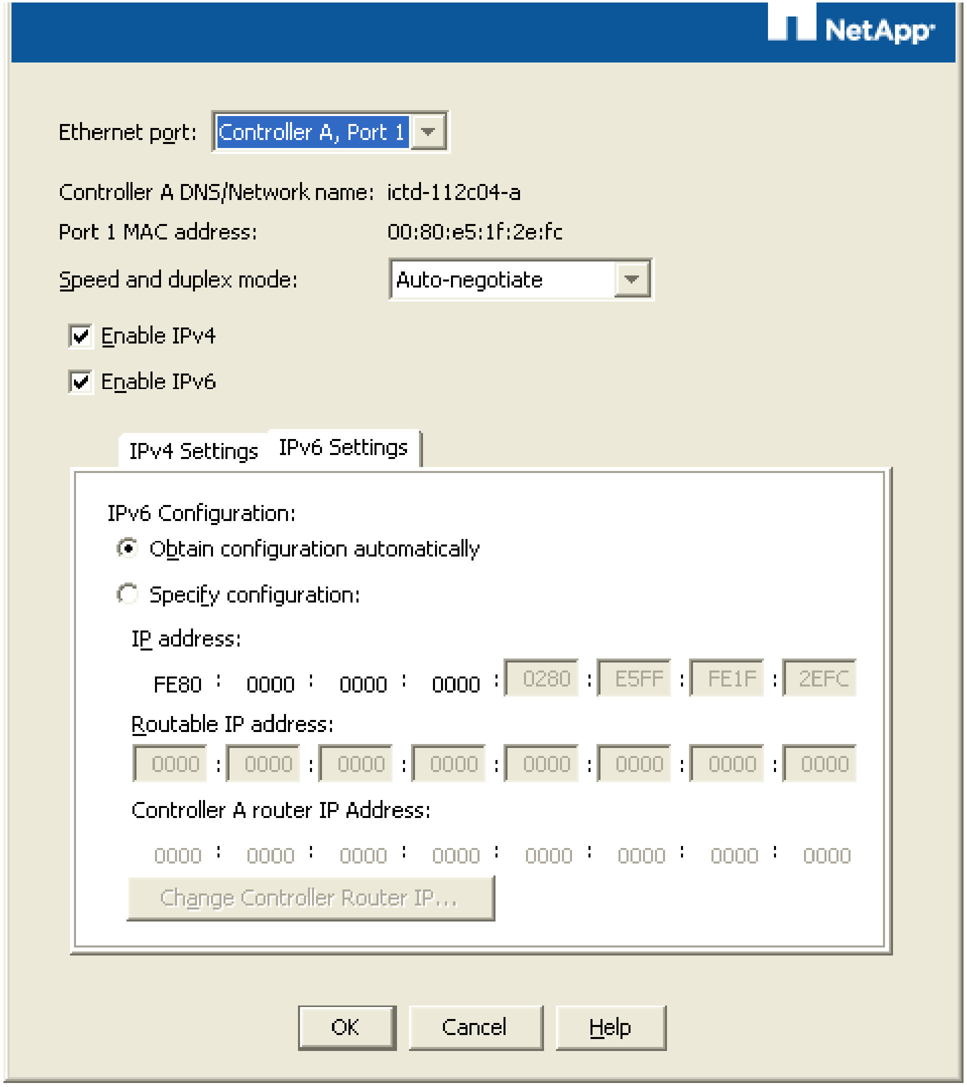
● Specify configuration:

IP address: 10 . 113 . 173 . 175

Subnet mask: 255 . 255 . 252 . 0

Controller A gateway:
10.113.172.1

Figure 7 Change Network Configuration Dialog with IPv6 Settings



Ethernet port: Controller A, Port 1

Controller A DNS/Network name: ictd-112c04-a

Port 1 MAC address: 00:80:e5:1f:2e:fc

Speed and duplex mode: Auto-negotiate

☑ Enable IPv4

☑ Enable IPv6

IPv6 Configuration:

● Obtain configuration automatically

○ Specify configuration:

IP address:

FE80 : 0000 : 0000 : 0000 : 0280 : E5FF : FE1F : 2EFC

Routable IP address:

0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

Controller A router IP Address:

0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0000

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 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 7 - 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 trays first, and then the controller-drive tray or controller tray).
- 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 "Naming the Storage Array" on page 41.
   - **No** – Go to "Procedure – Manually Adding a Storage Array" on page 38 (the storage array might reside outside the local sub-network).

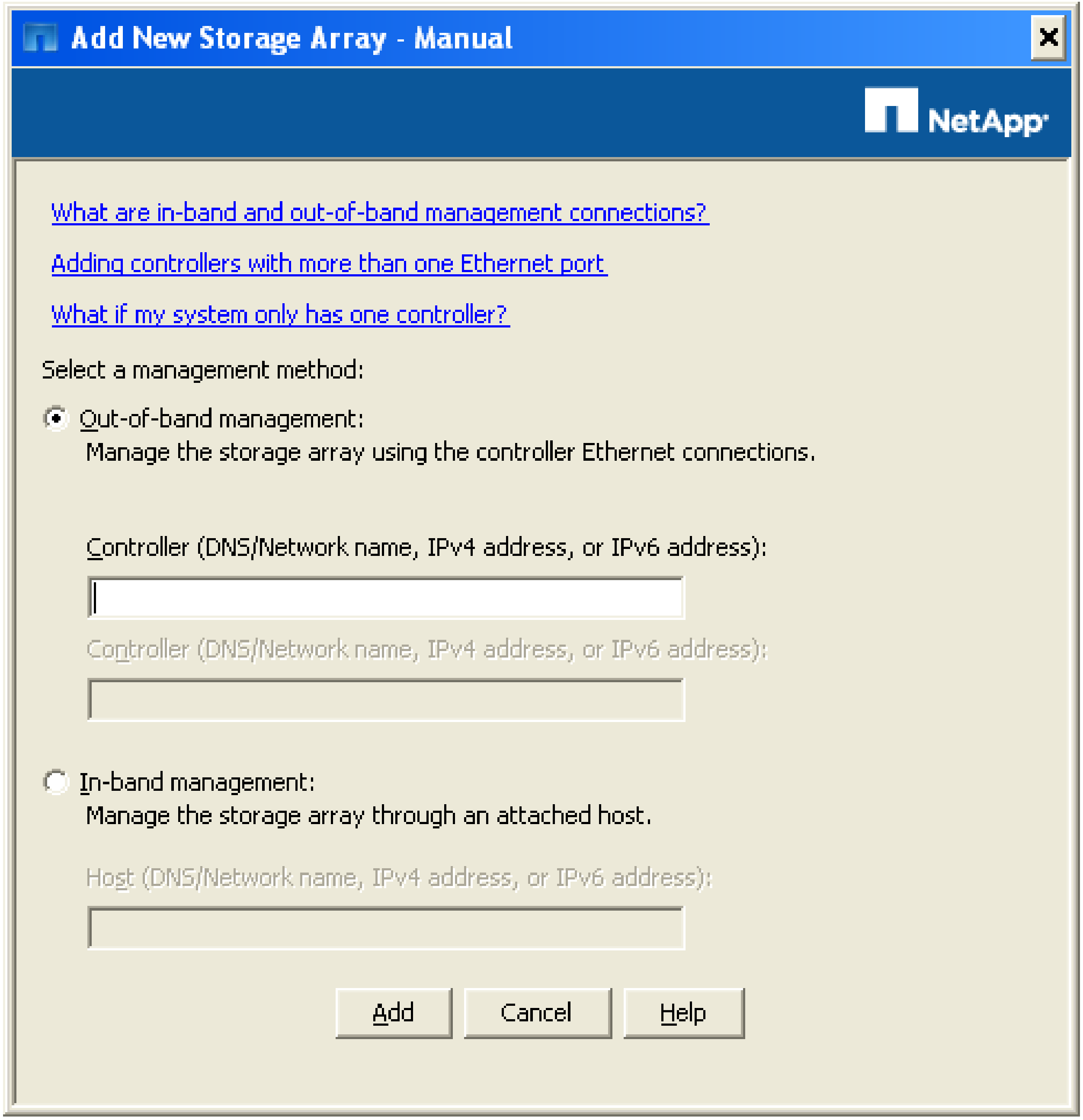
NOTE After adding the storage array, you can view or change the cache memory settings of the storage array. See "Changing the Cache Memory Settings" on page 53.

Procedure – Manually Adding a Storage Array

1. From the Enterprise Management Window, click the **Add Storage Arrays** link.

   The **Add New Storage Array – Manual** dialog appears. By default, the **Out-of-band management** radio button is selected.

Figure 8 Add New Storage Array – Manual Dialog



Add New Storage Array - Manual

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):

2. Select one of the following radio buttons, depending on the type of management you are using:

   — Out-of-band – Select the **Out-of-band management** radio button.

   — In-band – Select the **In-band management** radio button.

3. Manually enter the host names or the IP addresses of the controllers (out-of-band management method) or the host name or IP address of the host that is running the host-agent software (in-band management method), and click **Add**.

   The storage array appears in the Enterprise Management Window.

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 "Changing the Cache Memory Settings" on page 53.

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 Hosts**.
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 8 - 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.

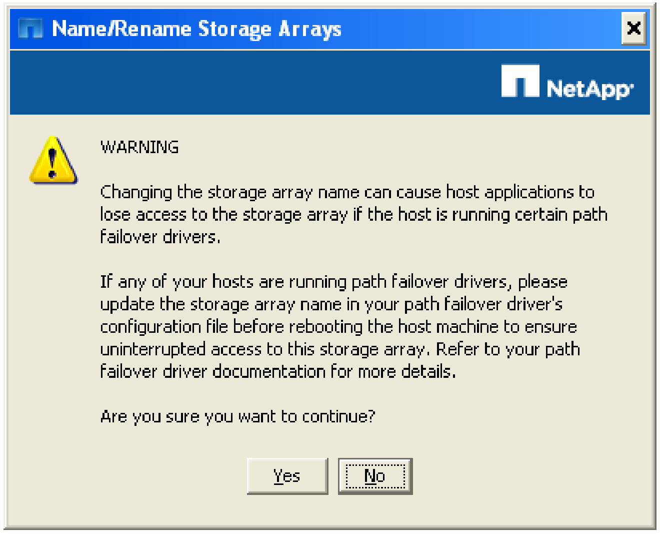
5. Repeat step 3 through step 4 for each unnamed storage array.

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:



WARNING

Changing the storage array name can cause host applications to lose access to the storage array if the host is running certain path failover drivers.

If any of your hosts are running path failover drivers, please update the storage array name in your path failover driver's configuration file before rebooting the host machine to ensure uninterrupted access to this storage array. Refer to your path failover driver documentation for more details.

Are you sure you want to continue?

8. Perform one of these actions:

   — **The host is not running any path failover drivers** – Click **Yes** to change the name of the storage array. Go to step 9 on page 42.

   — **The host is running a path failover driver** – Click **No**. Go to step 9 on page 42.

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 9 - Resolving Problems

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

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 **Hardware** 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 Adding Controller Information for the Partially Managed Storage Array on page 45.
   - **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.

Retrieving Trace Buffers

Use the 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 Technical Support representative.

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

- The World Wide Identifier (WWID) for the storage array.
- The serial number of each controller.
- A time stamp.
- The version number for the controller firmware.
- The version number for the management application programming interface (API).
- The model ID for the controller board.
- The collection status (success or failure) for each controller. (If the status is Failed, the reason for failure is noted, and no trace file exists for the failed controller.)

1. From the Array Management Window, select **Monitor >> Health >> 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 10 - Adding Controller Information for the Partially Managed Storage Array

NOTE You need to perform this step only 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 on page 39 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 Changing the Cache Memory Settings on page 53.

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

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

NOTE If you forget your password, you must contact your Technical Support 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 either **Edit >> Remove >> Storage Array** or **Edit >> Remove >> Management Connection**.
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

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

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 notification.

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 Technical Support representative; otherwise, delete the fields.

Filtering Tab

- Check the event severity that will trigger an alert notification for your storage array: **Critical**, **Warning**, **Informational**, and **Debug**. By default, all four settings are checked and that these settings will apply to all your storage arrays.

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 Technical Support representative, make sure that you select the **Event + Profile** or **Event + Support** choice in the Information to Send column. This additional information aids in troubleshooting your storage array. The **Event + Support** choice includes the profile.

SNMP Tab

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

Step 14 - Changing the Cache Memory Settings

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

Key Terms

cache memory

An area of random access memory (RAM) on the controller. This memory is dedicated to collecting and holding related data until a drive tray, a controller tray, or a controller-drive tray 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 either flushed from cache memory or written to the drives.
- When selecting the cache block size for your application, keep in mind that a smaller cache size is a good choice for file-system use or database-application use, but a larger cache size is a good choice for applications that generate sequential I/O, such as multimedia.
- During a controller failure, the data in the cache memory of the controller might be lost.
- To protect data in the cache memory, you can set a low percentage of unwritten data in the cache memory to trigger a flush to the drives. However, as the number of drive reads and drive writes increases, this setting decreases performance.
- When cache mirroring is enabled, if one controller in a controller tray or controller-drive tray fails, the second controller takes over. The surviving controller uses its mirrored version of the failed controller’s cache data to continue reading from and writing to the volumes previously managed by the failed controller.

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 **Hardware** tab.
4. Select controller A in the Hardware pane of the Array Management Window, and the **Properties** view appears in the right pane.
5. Scroll through the **Base** tab until you find the cache information and the cache backup device information.

Procedure – Changing the Storage Array Cache 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 **Storage >> 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.

   To enable copying of additional data while copying read operations data from the drives, select the **Dynamic cache read prefetch** 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.

ATTENTION Potential data loss – If you select this option and the storage array experiences a power failure, data loss can occur.

   — **Enable write caching with mirroring** – Mirrors data in the cache memory across two redundant controllers that have the same cache memory size.

7. Specify whether you want these settings to apply to all volumes or to any particular volumes in the storage array, and then 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 premium feature is either enabled or disabled.

A trial version of a premium feature allows you to use it for a limited amount of time and for a limited allowable value so that you can try it before you buy it. Each trial version of a premium feature requires a trial license. You can obtain a trial license for one or more of the following premium features:

- Snapshot groups
- Thin provisioning
- High performance tier
- Synchronous Mirroring (SM)

A trial license is valid for between 30 days and 90 days and it cannot be extended. Only one trial period is available for each premium feature. After you start a trial period, you cannot cancel it. You can purchase a license for a premium feature to activate it either before or at the end of the trial period. However, you must purchase the license before the trial ends for the premium feature to continue uninterrupted.

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** or click the **Use Key File** button in the **Enable a Premium Feature** pane.

   The associated **Select Feature Key File** dialog opens, which lets you select the generated key file.

6. Select the appropriate key file for the particular premium feature that you want to enable.
7. Click **OK**.

8. Click **Close** to close the **Select Feature Key File** dialog.

NOTE To check the status of a premium feature, select **Storage Array >> Premium Features**.

9. Repeat step 4 on page 55 through step 8 for each premium feature that you want to enable.

Procedure – Using a Trial Version of a Premium Feature

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. Make sure that the **Trials Available** check box is selected.

5. Scroll through the **Premium Features** list to display the premium feature that you want to try, and click the **Try Now** button.

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 (E2600 controller-drive tray, E2660 controller-drive tray, CE4900 controller-drive tray, E5400 controller-drive tray, E5460 controller-drive tray, or CE7900 controller tray) for instructions to obtain these world wide port names.

NOTE If you will not use storage partitions or you do not have the SANshare Storage Partitioning premium feature enabled on your storage array, you can skip the information about Things to Know – Host Groups and Things to Know – Storage Partitions,and go to either Procedure – Defining the Hosts on page 60 or Procedure – Defining the iSCSI Hosts on page 60.

Key Terms

host context agent

A software component that runs on each of the various storage array I/O hosts in the SAN in order to collect SAN topology-related information from the host where it is running and provide that information to each storage array attached to that host.

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, in most cases the storage management software does not know which host adapters are associated with which hosts. Only when the SMagent service runs on the host that is attached to a storage array can the storage management software associate HBA ports to that host.

For most cases, use the procedures below to associate each host with its specific host adapters.

NOTE By default, the host context agent automatically defines all attached hosts that are running SMagent in the mapping view of the Array Management Window with a default naming scheme, which you can modify to the needs of your configuration.

Things to Know – Host Groups

- A host group is a group (cluster) of two or more hosts that share access, in a storage partition, to specific volumes on the storage array. You can create an optional logical entity in the storage management software. You must create a host group only if you will use storage partitions.
- If you must define a host group, you can define it through the Define Hosts Wizard described in Procedure – Defining the Hosts on page 60.

Things to Know – Storage Partitions

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

- You *do not* need to create storage partitions if these conditions exist (see Figure 9):
  - You have only one attached host that accesses all of the volumes on the storage array.
  - You plan to have all of the attached hosts share access to all of the volumes in the storage array.

NOTE All of the attached hosts must have the same operating system (homogeneous), and you must have special software on the hosts (such as clustering software) to manage volume sharing and accessibility. This qualification does not, however, exclude the use of heterogeneous hosts (see Figure 11 on page 59)

- You *do* need to create storage partitions if these conditions exist:
  - You want certain hosts to access only certain volumes (see Figure 10 on page 59).
  - You have hosts with different operating systems (heterogeneous) attached in the same storage array. You must create a storage partition for each type of host (see Figure 11 on page 59).

Figure 9 Example of No Additional Storage Partitions Required

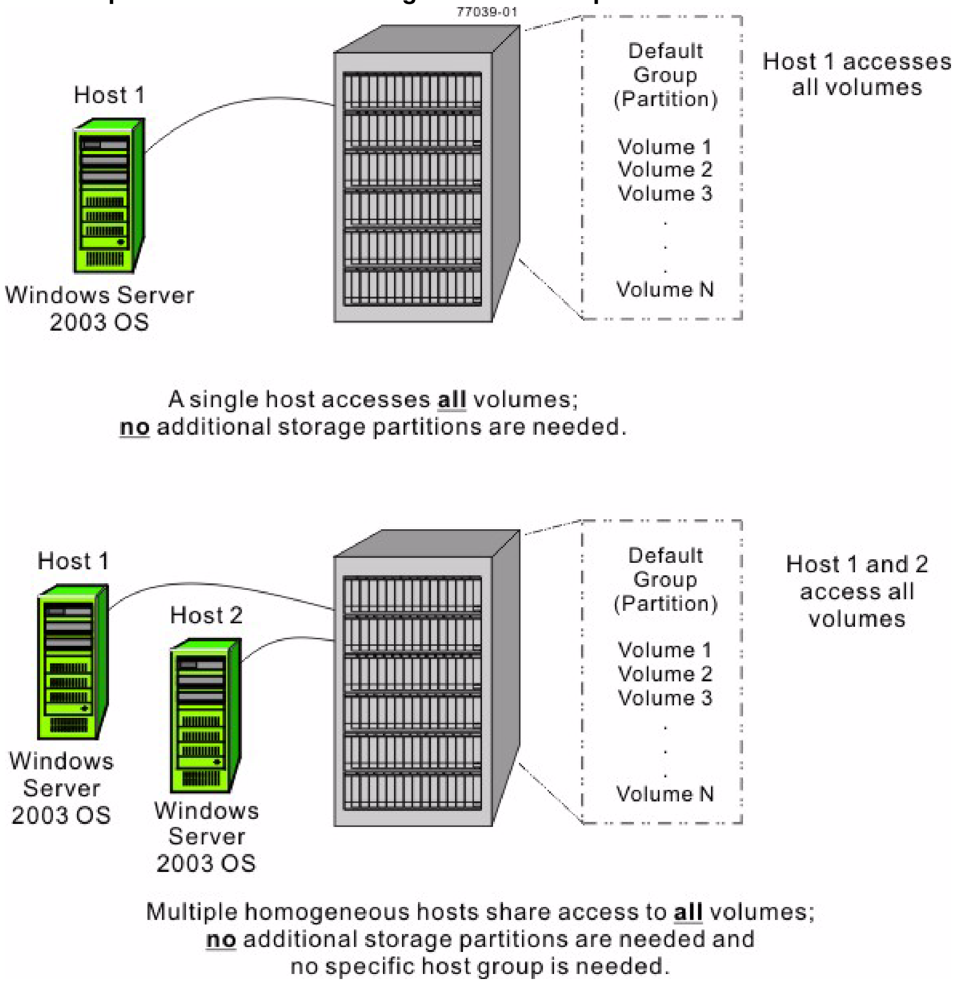
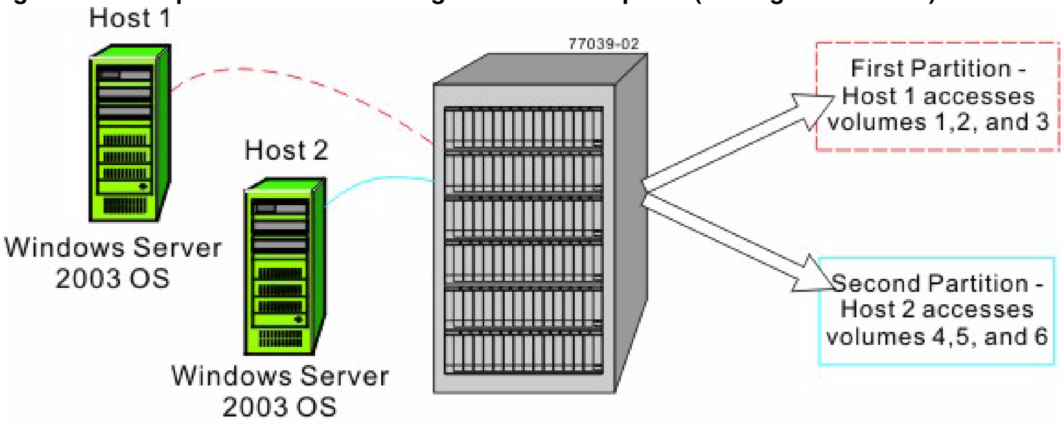
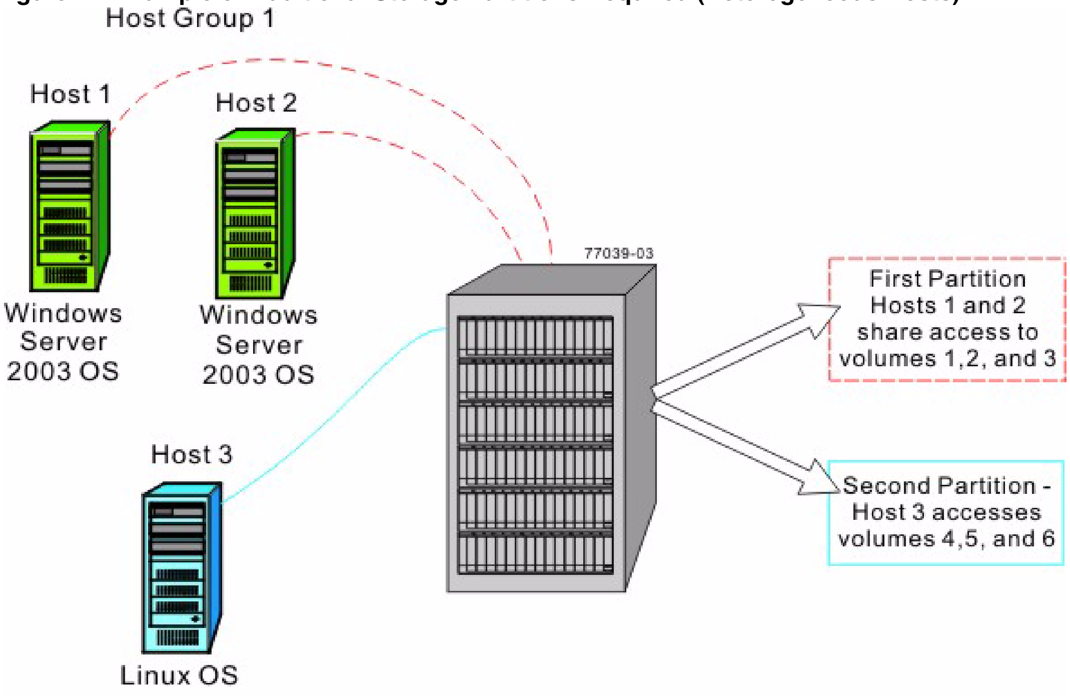

77039-01
Host 1
Windows Server 2003 OS
Default Group (Partition)
Volume 1
Volume 2
Volume 3
.
.
.
Volume N
Host 1 accesses all volumes
A single host accesses all volumes;
no additional storage partitions are needed.
Host 1
Windows Server 2003 OS
Host 2
Windows Server 2003 OS
Default Group (Partition)
Volume 1
Volume 2
Volume 3
.
.
.
Volume N
Host 1 and 2 access all volumes
Multiple homogeneous hosts share access to all volumes;
no additional storage partitions are needed and
no specific host group is needed.

Figure 10 Example of Additional Storage Partitions Required (Homogeneous Host)



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

Figure 11 Example of Additional Storage Partitions Required (Heterogeneous Hosts)



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

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. Does the storage array contain a 10Gb host interface card?

   — **Yes** – 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**, then go to step 5.

   — **No** –Go to step 5.

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

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

Although this section includes an overview of some premium features available with SANtricity ES Storage Manager. Refer to the *SANtricity ES Storage Manager Concepts Guide for Version 10.83* for a brief summary of all features and the online help for more detailed descriptions.

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.

Dynamic Disk Pool Volumes

Volumes created using new data protection methodology, which distinguishes RAID segments across a pool of disks.

free capacity

Unassigned space in a volume group or disk 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. Hot spare drives are used only in volume groups, not disk pools.

Redundant Array of Independent Disks (RAID)

CONTEXT [Storage System] A disk array in which part of the physical storage capacity is used to store redundant information about user data stored on the remainder of the storage capacity. The redundant information enables regeneration of user data in the event that one of the array's member disks or the access path to it fails.

Although it does not conform to this definition, disk striping is often referred to as RAID (RAID Level 0). (*The Dictionary of Storage Networking Terminology*)

storage partition

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

unconfigured capacity

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

volume

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

volume group

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

Things to Know – Using SATA Drives on an E2600 Controller-Drive Tray Running in Simplex Mode

You can use native SATA drives in an E2600 controller-drive tray that is running in simplex mode, that is, in a storage array when only one controller per controller-drive tray.

The SATA drives must support SMART Command Transfer (SCT) or the controller firmware locks them out.

If you receive an error message with the following drive status, you must replace those drives with native SATA drives that support SCT:

```
DRIVE_CAUSE_INCOMPATIBLE_SATA_DRIVE_SCT_UNSUPPORTED
```

If a single controller or a pair of controllers are in duplex mode and all the drives are native SATA drives, you might receive the following error status:

```
REC_ALL_DRIVES_BYPASSED_INCOMPATIBLE_NVSRAM
```

To resolve this issue, you must download an NVSRAM file that supports simplex mode. Because all the drives are bypassed, the client must use the new SYMbol command `loadControllerNVSRAMNoPassword`.

If you switch this controller-drive tray from simplex to duplex mode, you lose access to the native SATA drives.

Things to Know – Data Assurance

The Data Assurance (DA) premium feature checks for and corrects errors that might occur as data is communicated between a host and a storage array. DA is implemented using the SCSI direct-access block-device protection information model. DA creates error-checking information, such as cyclic redundancy checks (CRCs) and appends that information to each block of data. Any errors that might occur when a block of data is either transmitted or stored are then detected and corrected by checking the data with its error-checking information.

Only certain configurations of hardware, including DA-capable drives, controllers, and host interface cards (HICs), support the DA premium feature. When you install the DA premium feature on a storage array, SANtricity ES Storage Manager provides options to use DA with certain operations. For example, you can create a volume group that includes DA-capable drives, and then create a volume within that volume group that is DA-enabled. Other operations that use a DA-enabled volume have options to support the DA premium feature.

NOTE Neither iSCSI nor Infiniband host ports support the Data Assurance (DA) premium feature.

If you choose to create a DA-capable volume group, select the **Create a Data Assurance (DA) capable volume group** check box. This check box is enabled only when there is at least one DA-capable drive in the storage array and is, by default, selected if it is enabled.

When the DA premium feature is enabled, the DA Enabled column appears in the **Source volume** list in the **Create Copy Wizard – Introduction** dialog. If you choose to copy a DA-enabled source volume to a target volume that is not DA enabled, you are prompted to confirm your choice. The copy can be completed, but the resulting copy is not DA enabled.

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

You can verify that a drive contains DA-enabled volumes by checking that the **DA-enabled** volume property is set to **yes**.

Things to Know – Disk Pools and Disk Pool Volumes

The Dynamic Disk Pool feature is a way to deliver RAID protection and consistent performance. A disk pool is a set of drives that is logically grouped together in the storage array. The drives in each disk pool must be of the same physical drive type and drive media type, and they must be similar in size. As with a volume group, you can create one or more volumes in the disk pool. However, the disk pool is different from the volume group by the way the data is distributed across the drives that comprise the disk pool.

In a volume group, the data is distributed across the drives based on a RAID level. You can specify the RAID level when you create the volume group. The data for each volume is written sequentially across the set of drives that comprise the volume group.

In a disk pool, the storage management software distributes the data for each volume randomly across a set of drives that comprise the disk pool. Each disk pool must have a minimum of eleven drives. Although there is no limit on the maximum number of drives that can comprise a disk pool, the disk pool cannot contain more drives than the maximum limit for each storage array. The storage management software automatically configures the RAID level when you create the disk pool. You cannot set or change the RAID level of disk pools or the volumes in the disk pools.

NOTE Because disk pools can co-exist with volume groups, a storage array can contain both disk pools and volume groups.

Things to Know – Disk Pool Benefits

- **Easy to Create** – It is easy to create a disk pool in the storage management software. To create a disk pool, you just select the drives from a list of eligible drive candidates. After a disk pool is created, you create volumes. When you create disk pool volumes, the only attribute you must specify is the volume capacity.
- **Better Utilization of Drives** – When you add drives to a storage array, the storage management software automatically detects the drives and prompts you to create a single disk pool or multiple disk pools based on the drive type and the current configuration. If disk pools were previously defined, the storage management software provides the option of adding the compatible drives to an existing disk pool. When new drives are added to an existing disk pool, the storage management software automatically redistributes the data across the new capacity, which now includes the new drives that you added. The data in the volumes remain accessible when you add the drives to the disk pool. When you delete disk pool volumes, the capacity of those volumes is added to the total usable capacity of the disk pool and, therefore, can be reused.

NOTE You have the option to manually create a disk pool, if you prefer not to proceed with the automatic disk pool creation process.

- **Reduced Hot Spots** – A host might access some drives in the volume group for data more frequently than other drives because of the sequential manner in which the data is written to the drives. This frequency of access to drives creates hot spots in the volume group. In a disk pool, the hot spots are significantly reduced because of the random manner in which the data is spread across a large number of drives. The reduction of hot spots in the disk pool improves performance of the storage array.
- **Faster Reconstruction of Data** – Disk pools do not use hot spare drives for data protection like a volume group does. Instead of hot spare drives, disk pools use spare capacity within each drive that comprises the disk pool
- **Reduced Maintenance** – You can configure the storage management software to send alert notifications when the configured capacity of a disk pool is reaching a specified percentage of free capacity. Additionally, you do not need to manage any hot spare drives. You can replace a set of drives during a scheduled maintenance of the storage array.

For more information about disk pools, refer to the online help in the SANtricity ES Storage Manager.

Things to Know – Disk Pool Restrictions

- Dynamic Segment Sizing (DSS) is not supported for disk pools.
- You cannot change the RAID level of a disk pool. The storage management software automatically configures disk pools as RAID level 6.
- You cannot export a disk pool from a storage array or import the disk pool to a different storage array.
- All drive types (Fibre channel, SATA, SAS) in a disk pool must be the same.
- All drive media types in a disk pool must be the same. Solid State Disks (SSDs) are not supported.
- You can protect your disk pool with Full Disk Encryption (FDE), but the drive attributes must match. For example, FDE-enabled drives cannot be mixed with FDE-capable drives. You can mix FDE-capable and non FDE-capable drives, but the encryption abilities of the FDE drives cannot be used.
- You can use Data Assurance (DA) capabilities of a drive set in a disk pool if all drives match in their DA capabilities. However, you can use a drive set with mixed attributes, but the DA capabilities of the drive can not be used.
- If you downgrade the controller firmware version of a storage array that is configured with a disk pool, the volumes are lost and the drives are treated as unaffiliated with a disk pool.

For more information on disk pools, refer to the online help in the SANtricity ES Storage Manager.

Things to Know – Allocating Capacity

The drives in your storage array provide the physical storage capacity for your data. Before you can store data, you must configure the physical storage capacity into components, known as volume groups, disk pools, and volumes.

Volume groups and disk pools are a set of drives that the controller collects together. Volume groups and disk pools have these characteristics:

- They appear as one larger drive.
- They increase the performance of the storage array.
- They let the controller write to the multiple drives in the volume group or disk pool at the same time.
- They protect your data.
- They use Redundant Array of Independent Disks (RAID) technology.

The volume is a logical entity that your host uses to store data. Volume groups and disk pools can hold one or more volumes. You create volumes from free capacity in the volume group or disk pool.

Keep the following in mind as you configure your storage array capacity:

- The operating system (OS) for your host might have specified limits about how many volumes the host can access. Keep these limits in mind when you create volumes for a particular host.
- Make sure that some non-configured capacity stays in the form of one or more unassigned drives. Keep some unconfigured capacity so that you have capacity available for additions or changes to your configuration. You might need unconfigured capacity for one of these modifications:
  - Creating one or more snapshot (legacy) volumes
  - Increase free capacity of a volume group or a disk pool
  - Expanding a snapshot (legacy) repository volume
  - Configuring one or more hot spare drives

NOTE Hot spare drives apply only to volume groups. Disk Pools do not use hot spare drives.

- You can create volumes from either unconfigured capacity or free capacity on an existing volume group.
  - — If you create a volume from unconfigured capacity, you must first specify the parameters for a new volume group or disk pool (RAID level and the number of drives required) before you specify the parameters for the first volume on the new volume group or disk pool.
  - — If you create a volume from free capacity, you have to specify the parameters of only the volume, because the volume group or disk pool already exists.
- Mixing drives with different media types or interface types within one volume group or disk pool is not permitted. For example, you cannot mix Serial Attached SCSI (SAS) drives with either SATA or Fibre Channel drives, and you cannot mix hard drives with Solid State Disks (SSDs).
- If you are adding capacity to a Data Assurance (DA) -capable volume group or disk pool, use only drives that are DA capable. If you add a drive or drives that are not DA-capable, the volume group or disk pool no longer has DA capabilities, and you no longer can enable DA on newly created volumes within the volume group or disk pool. The DA Capable column in the **Available drives** list shows the DA capabilities of each listed drive.
- If you are adding capacity to a volume group or disk pool that is not DA capable, do not use drives that are DA capable because the volume group or disk 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.
- If you are adding capacity to a Full Disk Encryption (FDE) -capable volume group or disk pool, use only drives that are FDE capable. If you add a drive or drives that are not FDE-capable, the volume group or disk pool no longer has FDE capabilities, and you no longer can enable FDE on newly created volumes within the volume group or disk pool.
- If you are adding capacity to a volume group or disk pool that is not FDE capable, do not use drives that are FDE capable because the volume group or disk pool cannot take advantage of the capabilities of FDE-capable drives.

Things to Know – Volume Groups and Volumes

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

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

- While creating volume groups, you must make sure that the drives that comprise the volume group are located in different drive trays. This method of creating volume groups is called tray loss protection. Tray loss protection guarantees accessibility to the data on the volumes in a volume group if a total loss of communication occurs with a single drive tray. Communication loss might occur due to loss of power to the drive tray or failure of the drive tray ESMs.
- The RAID levels supported are RAID Level 0, RAID Level 1, RAID Level 3, RAID Level 5, RAID Level 6, and RAID Level 10 (1 + 0).
  - — RAID Level 0 provides no data redundancy.

- RAID Level 10 is not a separate RAID level choice but is supported when you create a RAID Level 1 volume group that consists of four or more drives.
- You can assign RAID Level 1 only to volume groups with an even number of drives.
- You can assign RAID Level 3 or RAID Level 5 only to volume groups with three or more drives.
- You can assign RAID Level 6 only to volume groups with five or more drives.

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

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

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

Things to Know – Hot Spare Drives

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

Things to Know – Full Disk Encryption

Drive Security and Enterprise Security 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* full disk encryption (FDE) drives. A security-capable FDE drive encrypts data during writes and decrypts data during reads. Each security-capable drive has a unique drive encryption key.

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

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

You can view the 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 security disabled
- Read/Write Accessible – Security locked or security unlocked

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

- Security-capable
- Secure

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

Table 9 Volume Group Security Properties

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

When the 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**
- **Import Key**
- **Save Security Key**
- **Unlock Drives**
- **Validate Key**

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

If you have created a security key for the storage array, the **Create Security Key** option is inactive with a check mark to the left. The **Change Security Key** option, the **Save Security Key** option, and the **Validate Security Key** option 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 **Volume Group** menu. The **Secure Drives** option is active if these conditions are true:

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

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

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

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

The storage array password protects a storage array from potentially destructive operations by unauthorized users. The storage array password is independent from the 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 **Create Storage**.

4. Choose the applicable configuration task:

   — **Automatic configuration** – This method either uses the drives to provision disk pools so that data can be distributed for quick reconstruction or creates volume groups with equal-sized capacity volumes and also automatically assigns appropriate hot spare drive protection. Use this method if you do not have unique capacity requirements for each disk pool or volume group, or you want a quick method to configure disk pools or volume groups, volumes, and hot spare drives. You can choose from a list of suggested configurations, or you can create your own custom configuration.

   — **Manual configuration** – This method creates storage manually by selecting one of the following options: **Create disk pool**, **Create volume groups and volumes**, or **Configure hot spares (drives only)**.

   Create disk pool – This method allows you to select a collection of drives to provision into a disk pool. Data is distributed over a larger set of drives for quick reconstruction and recovery.

   Create volume groups and volumes – This method creates one volume at a time but gives you more control over the volume group and volume parameters (such as RAID level, volume 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 map the volume groups, volumes, and hot spare drives, perform one of these actions depending on your storage partition requirements. Refer to the on-screen instructions and the online help topics for more information.

   — **No storage partition is required, and you selected the automatic configuration method** – Go to step 6 on page 69.

   — **No storage partition is required, and you selected the manual configuration method** – Verify whether all volumes are mapped to the Default Group, and go to step 8 on page 69.

   — **A storage partition is required** – Go to step 7 on page 69.

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 must select 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 partition.

   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 `cxtxdx` is the device name of each volume.

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

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

NOTE After you configure the volume, you can change the cache memory settings of the volume. See “Procedure – Changing the Volume Cache Memory Settings” on page 54.

Step 18 - Downloading the Drive and ATA Translator Firmware for SATA Drives and the DE6900 Drive Tray

Each SATA drive in a DE6900 drive tray is connected to a corresponding ATA translator (12 to a drawer). The ATA translator provides *Fibre Channel (FC)* protocol to *Serial Advanced Technology Attachment (SATA)* protocol translation for the SATA drives in the storage array.

Use the **Drive/ATA Translator Firmware** option to transfer a downloadable *firmware* file to the drives and the Advanced Technology Attachment (ATA) translators in the *storage array* only if the drives and the ATA translators in the storage array are experiencing firmware-related limitations or performance issues. Obtain drive and ATA translator firmware only from your storage supplier.

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

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

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

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

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

ATTENTION Possible damage to drives and loss of data – Do not make any configuration changes to the storage array while downloading firmware files.

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

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

1. From the Array Management Window, select **Upgrade >> Drive Firmware**.

   The **Download Drive Firmware - Introduction** dialog appears.

2. Follow the directions on each dialog, and click **Next** to move to the next dialog.

   Each dialog has context-sensitive help. Click **Help** to view the information applicable for that particular dialog.

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

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

Procedure – Starting the Download Process

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

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

Procedure – Selecting the Drive and the ATA Translator Firmware

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

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

NOTE Selecting more than one firmware file to update the firmware of the same drive or ATA translator might result in a file-conflict error. If a file-conflict error occurs, an error dialog appears. To resolve this error, click **OK**, and remove all other firmware files except the one that you want to use for updating the firmware of the drive or the ATA translator. To remove a firmware file, select the firmware file in the Selected packages area, and click **Remove**.

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

Procedure – Updating the Firmware

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

1. Select the drives and ATA translators for which you want to download the firmware.

   — **For one or more drives and ATA translators** – In the Select drives area, select the drive and ATA translator names.

   — **For all compatible drives and ATA translators listed in the dialog** – Click **Select All**.

2. Click **Finish**.

   The **Confirm Download** dialog appears.

3. To start the firmware download, type `yes` in the text box.
4. Click **OK**.

Procedure – Monitoring the Progress of the Download

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

ATTENTION Possible loss of access to data or data loss – Stopping a firmware download might result in drive unavailability or data loss.

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

NOTE Each firmware download can take several minutes to complete.

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

NOTE A drive or an ATA translator does not show in the Drives updated area until a firmware download is attempted or the firmware download process is stopped.

2. To stop the firmware download in progress, click **Stop**.

   Any firmware downloads currently in progress are completed. Any drives or ATA translators that have attempted firmware downloads show their individual status. Any remaining drives or ATA translators are listed with a status of Not attempted.

3. If you want to save a text report of the progress summary, click **Save As**.

   The report saves with a default `.txt` file extension. If you want to change the file extension or directory, change the parameters in the **Save As** dialog.

4. Perform one of these actions:

   — **To close the Drive Firmware Download Wizard** – Click **Close**.

   — **To start the wizard again** – Click **Transfer More**.

Regulatory Compliance Statements

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his/her own expense.

NetApp, Inc. is not responsible for any radio or television interference caused by unauthorized modification of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by NetApp. It is the user's responsibility to correct interference caused by such unauthorized modification, substitution, or attachment.

Laser Products Statement

This equipment uses Small Form-factor Pluggable (SFP) optical transceivers, which are unmodified Class 1 laser products pursuant to 21 CFR, Subchapter J, Section 1040.10. All optical transceivers used with this product are required to be 21 CFR certified Class 1 laser products. For outside the USA, this equipment has been tested and found compliant with Class 1 laser product requirements contained in European Normalization standard EN 60825-1 1994+A11. Class 1 levels of laser radiation are not considered to be hazardous and are considered safe based upon current medical knowledge. This class includes all lasers or laser systems which cannot emit levels of optical radiation above the exposure limits for the eye under any exposure conditions inherent in the design of the laser products.

NetApp, Inc. is not responsible for any damage or injury caused by unauthorized modification of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by NetApp. It is the user's responsibility to correct interference caused by such unauthorized modification, substitution, or attachment.

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classé A respecte toutes les exigences du Règlement sure le matèriel brouilleur du Canada.

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）基準に適合しております。

従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。

取扱説明書に従って正しい取り扱いをして下さい。

警告使用者：　這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

52900-00A