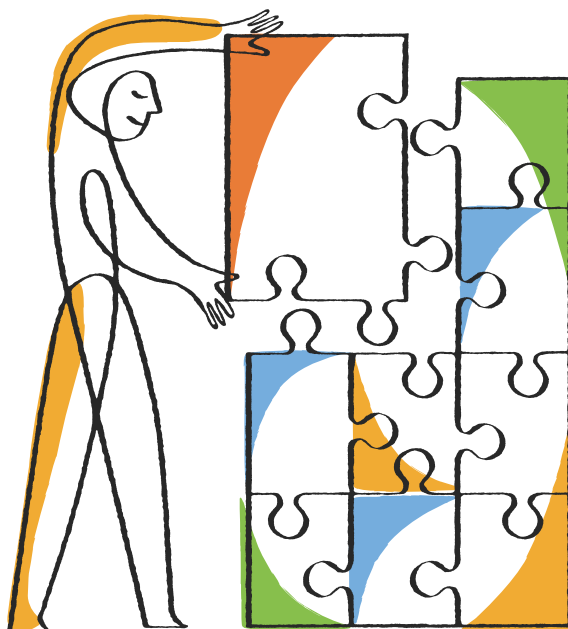# NetApp® E-Series Storage Systems

Initial Configuration and Software Installation for SANtricity® Storage Manager 11.10

Table of Contents

About This Guide

The information in this guide provides the conceptual framework necessary to understand the failover drivers used with SANtricity® Storage Manager Version 11.10. To access this software, go to the NetApp Support Site at support.netapp.com.

Some software features described in this document might not be available for your NetApp E-Series Storage System. For questions about available features, contact your NetApp account representative.

NOTE The SANtricity Storage Manager software is also referred to as the storage management software.

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 and use SANtricity Storage Manager software.

Key Terms

Things to Know – Management Method

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

Key Terms

access volume

in-band management

out-of-band management

stateless address autoconfiguration

storage manager event monitor

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.

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. The SMagent must be installed for this method to work correctly.

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. This is the recommended management method.

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.

storage manager event monitor

An application in the storage management software that monitors all activities on a storage array. The Event Monitor runs continuously on a host or storage management station. The Storage Manager Event Monitor is also referred to as the Event Monitor and the Persistent Monitor.

Things to Know – Management Method

NOTE If you use the out-of-band management method but do not have a DHCP server, you need to manually configure your controller IP addresses. See "Step 6 – Manually Configuring the Controllers" for details.

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

NOTE The example in Figure 1 shows the Client running on a second host. However, the Client can run on the same host as the Agent.

Figure 1. In-Band Management Topology
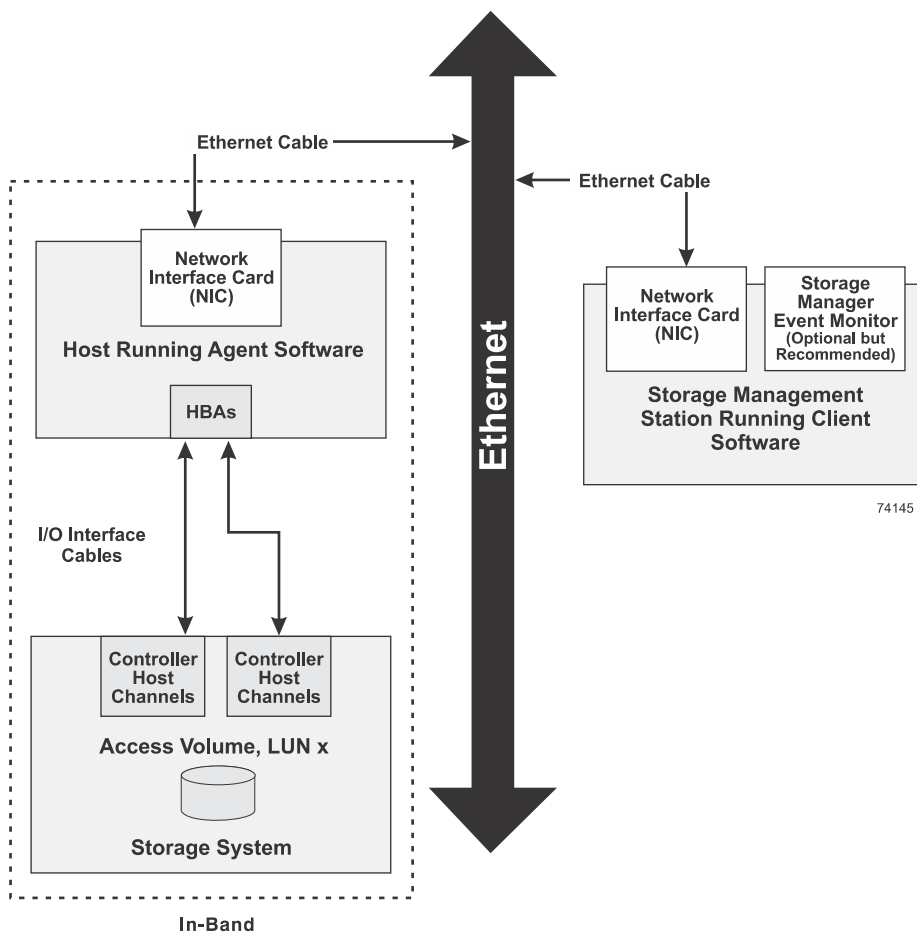
Figure 2. Out-of-Band Management Topology
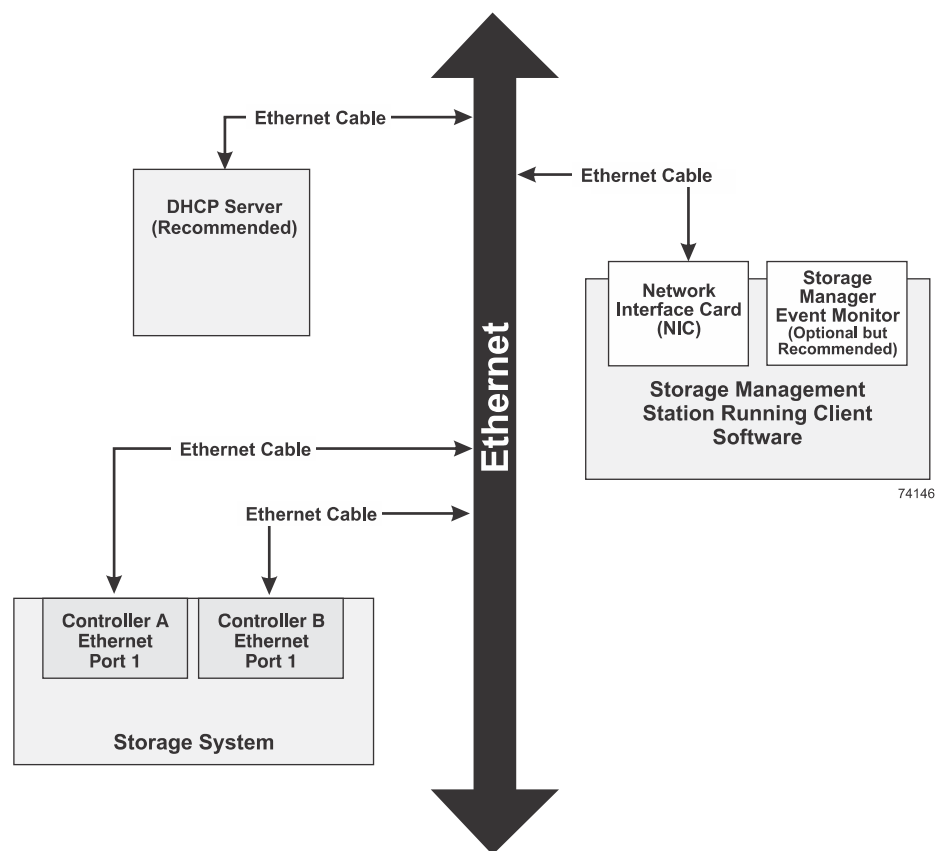
Things to Know – In-Band and Out-of-Band Requirements

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

Management Method	Requirements	Advantages	Disadvantages
All Out-of-band methods	Connect separate Ethernet cables to each controller.	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 I/O path bandwidth for storage array management functions.	Refer to the following three types of out-of-band methods.
Out-of-band *without* a DHCP server	Manually configure the network settings on the controllers. See "Step 6 – Manually Configuring the Controllers" for more information.		You must manually configure the network settings on the controllers. Ethernet cables are required.
Out-of-band – IPv6 stateless address auto-configuration *without* a DHCP server (IPv6 networks only)	Connect 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.	Ethernet cables are required. A router is required.

Management Method	Requirements	Advantages	Disadvantages
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 using your DHCP server. Alternatively, the SANtricity Storage Manager AMW can be used to set the IP addresses after the storage array has been discovered. 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*. 	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 special Access Volume to communicate with the host. This method does not use the SAS, Fibre Channel or iSCSI bandwidth for storage array management functions.	Ethernet cables are required.
In-band	Install the host agent software (SMagent) on at least one of the I/O-attached hosts. The host-agent software, which is included with the storage management software, manages the storage array through the data path from an I/O-attached host or an Ethernet connection from a storage management station to the I/O-attached host that is running the host-agent software. The in-band method requires a special access volume to communicate between the host and the storage array. 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. This method is not supported on InfiniBand systems. This method is not supported on some OSes (VMware, OS X).

Step 2 – Installing the SANtricity Storage Manager Software

This section provides information on key management software terms, overviews interoperability and system requirements, and describes how to use the installation wizard to install SANtricity Storage Manager software (hereinafter referred to as the storage management software). The separate native installation packages are supplied with SANtricity Storage Manager in the `native` directory. Refer to NetApp Support Site at support.netapp.com for updates.

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

If you are running a Windows Server Core version, make sure that you have performed the procedures in "Step 3 – Setting Up the Storage Array for Windows Server Core Editions." The specific steps for installing the storage management software are in "Server Core Setup Procedure – Installing the Storage Management Software."

If you are not running Windows Server Core, install SANtricity Storage Manager by performing the steps in "Procedure – Installing the SANtricity Storage Manager Software."

Key Terms

Things to Know – Host Operating Systems

Things to Know – Storage Management Software Components

Procedure – Installing the SANtricity Storage Manager Software

Key Terms

client

host

multi-path driver, failover driver

storage management software

storage management station

storage manager event monitor

client

1. An intelligent device or system that requests services from other intelligent devices, systems, or appliances.

2. An asymmetric relationship with a second party (a server) in which the client initiates requests and the server responds to those requests.

host

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

multi-path driver, failover 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. Multi-path drivers might require installation on the I/O attached servers, or they might be part of the host OS.

storage management software

Software that saves data from a network to a physical and logical organization of drives. The data is spread out across multiple drives, copied (physically or virtually) to another location, or both, for failure protection and redundancy.

storage management station

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

storage manager event monitor

An application in the storage management software that monitors all activities on a storage array. The Event Monitor runs continuously on a host or storage management station. The Storage Manager Event Monitor is also referred to as the Event Monitor and the Persistent Monitor.

Things to Know – Host Operating Systems

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

NOTE For HBA information specific to your operating system, refer to the NetApp Interoperability Matrix at support.netapp.com/matrix.

NOTE For updates in OS versions supported after publication of this document, refer to the NetApp Support Site at support.netapp.com for updates.

Table 2. Operating System Version or Edition Requirements

Operating System	System and Version or Edition
AIX (FC only)	**OS Versions for I/O attach hosts**: • 6.1 TL8 • 7.1 TL2 Full Client, Agent, and util support is available, as well as both in-band and out-of-band management. **Processor supported**: • IBM POWER^{TM} 5 and newer **I/O Path Fail-over**: Native MPIO (non-ALUA) --- **NOTE** For MPIO to recognize the storage, you must make sure your NVSRAM is the latest version available. Obtain the latest version of the NVSRAM from NetApp Support Site at support.netapp.com. --- • AIX 6.1 TL8 • AIX 7.1 TL2 **SANboot support**: Yes (For more information, refer to "Appendix B: Boot Device Installation.")
Linux	**OS Versions for I/O attach hosts**: • Linux Red Hat 5.9, 5.10 • Linux Red Hat 6.3, 6.4, 6.5 • CentOS 6.3, 6.4 • SUSE Linux Enterprise Server 10.4 • SUSE Linux Enterprise Server 11.2, 11.3 Full Client, Agent, and util support is available, as well as both in-band and out-of-band management **Processors supported**: • Intel Xeon 64-bit • AMD Opteron 64-bit **JRE level:** 7u45 **I/O Path Fail-over**: • **DM-MP (DMMP - RDAC handler)**: SUSE Linux Enterprise Server 11.3, 11.2; Linux Red Hat 6.5, 6.4, 6.3 Depending on your operating system release level, additional steps might be required to enable DM-MP with ALUA support. Refer to NetApp Support Site at support.netapp.com for updates. Refer to the *Failover Drivers Guide* for detailed instructions about applying these patches. • **MPP (MPP - RDAC driver)**: Linux Red Hat 6.5, 6.4, 6.3, 5.10, 5.9, SUSE Linux Enterprise Server 11.3, 11.2, 10.4 **SANboot supported**: Where supported by the HBA. For more information, refer to "Appendix B: Boot Device Installation.") --- **NOTE** No SANboot supported for iSCSI SWI. ---

Operating System	System and Version or Edition
Linux (InfiniBand)	**OS Versions for I/O attach hosts**: ▪ Linux Red Hat 5.10 ▪ Linux Red Hat 6.4 ▪ SUSE Linux Enterprise Server 11.3 Only out-of-band management support is available; any supported version from previous section. **Processors supported**: ▪ Intel Xeon 64-bit ▪ AMD Opteron 64-bit **JRE level:** 7u45 **I/O Path Fail-over**: DM-MP ALUA drivers, which will require a maintenance kernel. **NOTE** Depending on your operating system release level, additional steps might be required to enable DM-MP with ALUA support. Refer to NetApp Support Site at support.netapp.com for updates. Refer to the *Failover Drivers Guide* for detailed instructions about applying these patches. **SANboot supported**: No.
Mac OS X	**OS Versions for I/O attach hosts**: ▪ Mac OS X 10.7 ▪ Mac OS X 10.8 No Client, Agent, or Util support, and only out-of-band management is supported through another supported OS or guest OS. This is an I/O attach only solution with no SANtricity client support. **I/O Path Fail-over**: ATTO driver using TPGS with ALUA. **SANboot support**: No
Solaris SPARC-based system (FC only)	**OS Versions for I/O attach hosts**: ▪ Solaris 11.1 (FC and iSCSI) ▪ Solaris 10 u11 (FC only) 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:** 7u45 or later **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 u11 (FC only) - Solaris 11.1 (FC and iSCSI) 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:** 7u45 **I/O Path Fail-over**: MPxIO
VMware	**OS Versions for I/O attach hosts**: - 5.0 u2 - 5.1 u1 - 5.5 No Client, Agent, or Util support, and only out-of-band management is supported through another supported OS or a guest OS. **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 Storage Array Type Plug-in (SATP) -ALUA **SANboot supported**: On Fibre Channel and SAS only. (For more information, refer to "Appendix B: Boot Device Installation.") **NOTE** No SANboot supported for iSCSI SWI.

Operating System	System and Version or Edition
Windows Server 2012	**OS Editions for I/O attach hosts**: - Foundation Server and Core - Windows Server 2012 - Essentials - Standard Server and Core - Datacenter Server and Core **NOTE** Server Core versions have different installation instructions as they allow only the storage management command line interface (SMcli). **Hypervisor OS for I/O attach**: Windows Server 2012 Hyper-V, Windows Server 2012 R2 Hyper-V **OS Versions for the GUI client only (no I/O attach):** - Windows 8 **Processors supported**: - Intel Xeon 64-bit - Intel Xeon 32-bit (client only; no I/O attach) - AMD Opteron 64-bit - AMD Opteron 32-bit (client only; no I/O attach) **JRE level:** 7u45 or later **I/O Path Fail-over**: Microsoft MPIO using the NetApp DSM with ALUA support **SANboot supported**: Where supported by the HBA. (For more information, refer to "Appendix B: Boot Device Installation.") **NOTE** No SANboot supported for iSCSI SWI.

Operating System	System and Version or Edition
Windows Server 2008 R2 SP1 (64-bit only), Hyper-V	**OS Editions for I/O attach hosts**: ■ Standard Server and Core ■ Enterprise Server and Core ■ Datacenter Server and Core ■ Foundation Server and Core ■ Windows Storage Server **Hypervisor OS for I/O attach:** ■ Hyper-V Server 2008 R2 SP1 (standalone); out-of-band management method only supported ■ Windows Server 2008 R2 SP1 Hyper-V (an add-on to Windows Server 2008 **OS Versions for the GUI client only (no I/O attach):** ■ Windows Vista ■ Windows 7 ■ Windows 8 ■ Windows 8.1 **Processors supported**: ■ Intel Xeon 64-bit ■ Intel Xeon 32-bit (no I/O attach) ■ AMD Opteron 64-bit ■ AMD Opteron 32-bit (no I/O attach) **JRE level:** 7u45 **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 Server 2008 R2	434 MB	—
Windows Server 2012	434 MB	—
Linux	390 MB	—
Solaris	540 MB	—
AIX	525 MB	—

NOTE The minimum RAM requirement for the management host where SANtricity Storage Manager will be installed is 2 GB for the Java Runtime Engine.

Things to Know – Storage Management Software Components

This section provides information about installing the storage management software.

Client – This package contains both the Graphical User Interface (GUI) and the Command Line Interface (CLI) for managing the storage array. This package also contains a monitor service that sends alerts when a critical problem exists with the storage array.

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"). This package is required for in-band management.

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

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

NOTE The Microsoft Virtual Disk Service (VDS) and Volume Shadow Copy Service (VSS) providers might be part of the SANtricity Storage Manager package for Windows Server.

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 During the client installation, you might be asked whether you want to start the event monitor. Start the monitor on only one host that runs continuously. If you do not have event monitor running on one host, you will not receive critical alert notifications and you will not have access to the AutoSupport feature. If you start the monitor on more than one host, you receive duplicate alert notifications about problems with the storage array. If you install SANtricity components on more than one host and are not asked about the event monitor, it is recommended that you verify that the monitor is active on only one of the systems.

Figure 3. Software Configurations

**Host - Also acting as
an agent (in-band path)**

**Host - Also acting as a
monitor and an agent
(in-band path)**

**Host -
Also acting as
monitor**

Host - I/O only

**Management
Station**

☐ Client
☑ Utilities
☑ Agent
☑ Failover Driver
☐ Java Access Bridge

☐ Client
☑ Utilities
☐ Agent
☑ Failover Driver
☐ Java Access Bridge

☑ Client with Monitor
☑ Utilities
☐ Agent
☑ Failover Driver
☐ Java Access Bridge

☑ Client with Monitor
☑ Utilities
☑ Agent
☑ Failover Driver
☐ Java Access Bridge

☑ Client
☐ Utilities
☐ Agent
☐ Failover Driver
☑ Java Access Bridge
   (available only on the Windows OS)

77039-09

Storage Array

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 • Storage Manager Event Monitor **NOTE** Linux OS automatically installs the Event Monitor when you install the storage management software.	• Click **No** to the prompt, Automatically start Monitor? • You must choose **Custom** if you want to install the Java Access Bridge software.

Machine	Minimum Software Required	Installation Package (Choose One) (See the tables that follow)	Notes
Management station with the Storage Manager Event Monitor always running	Client	- Typical Installation - Management Station - Custom	- Click **Yes** to the prompt, Automatically start Monitor? - You must choose **Custom** if you want to install the Java Access Bridge software.
Host (I/O only)	- 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	- Client (either on this host or on a machine with network access to this host) - Utilities - Agent - Failover driver	- Typical Installation - Host - Custom	Click **No** to the prompt, Automatically start Monitor?
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 components)	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 Components That Are Supported on Each Operating System

Operating System	Client	Utilities	Agent	Failover	JAB
Windows Server 2008 R2 SP1 (64 bit only), Hyper-V	X	X	X	X[a]	X
Windows Server 2012, Hyper-V	X	X	X	X	X
Windows 7, Windows 8	X	—	—	—	X
VMware	X	—[b]	—	X[c]	—
Red Hat Enterprise Linux 5.9, 5.10, 6.3, 6.4, 6.5 SUSE Linux Enterprise 10SP2, 11SP3, 11SP4 (all 64-bit)	X	X	X	X[d]	—
DM-MP RDAC handler Red Hat Enterprise Linux 6.3, 6.4, 6.5 SUSE Linux Enterprise 11SP3, 11SP4 CentOS 6.3, 6.4 (all 64-bit)	X	X	X	X[e]	
Red Hat 6.1 Client SUSE Linux Enterprise 11.1 (InfiniBand)	X	—	—	X	—
Solaris Sparc (FC only)	X	X	X	X	—
Solaris x86 (FC only)	X	X	X	X	—
Mac 10.6 and 10.7	—	—	—	X	—
HP-UX 11.31 (FC only)	X	X	X	X[f]	—

[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, refer to the *Failover Drivers Guide*.

[d] NetApp MPP RDAC failover driver; Can be installed during SANtricity Storage Manager installation.

[e] DM-MP RDAC failover native in Linux distribution.

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

Procedure – Installing the SANtricity Storage Manager Software

NOTE Refer to NetApp Support Site at support.netapp.com for information about how the product is distributed.

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

1. If you are installing from a DVD, insert the DVD in the DVD drive, otherwise, go to step .

   Depending on your operating system, a program autoplays and shows a menu with installation selections. If the menu does not appear, you must manually open the `install` folder and locate the installation package needed.

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.

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

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

NOTE Make sure that your screen display is correctly set to run commands.

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

Procedure – Installing the Storage Manager Native Packages on the Linux OS

NOTE Before you install the client software, you must install the runtime software. Installing the storage manager packages is required for both hosts and storage management stations. There are two install packages available, depending on whether your Linux server is 32-bit or 64-bit:

- 32-bit server – Install the SMIA-Linux package.
- 64-bit server – Install the SMIA-LinuxX64 package.

In these procedures, you must enter commands to install the applicable software packages. After each initial command, the software installation starts. When the installation has completed, a message indicates that the installation was successful. Then, you are returned to the command prompt.

1. To install the packages, type the following commands in the sequence shown, and press **Enter** after each command.

   In the table that follows, *<mount-point>* is a placeholder for the mount point for the disc, and *<SM*-package>* is a placeholder for the package name of each storage manager package.

Package	
Runtime	rpm -ivh /<mount-point>/install/native/<SMruntime-package>.rpm
ESM	rpm -ivh /<mount-point>/install/native/<SMesm-package>.rpm
Client	rpm -ivh /<mount-point>/install/native/<SMclient-package>.rpm
Utilities	rpm -ivh /<mount-point>/install/native/<SMutil-package>.rpm
Agent	rpm -ivh /<mount-point>/install/native/<SMagent-package>.rpm

2. To install RDAC, you need to unzip the `RDAC tar.gz` file and untar the RDAC tar file by typing the command **tar -zxvf <filename>** and pressing **Enter**.

3. Go to the Linux RDAC directory `cd linuxrdac`.

4. If you have a previous RDAC version, type the command **Make uninstall** and press **Enter**.

5. To remove the old driver modules in that directory, type the command **make clean** and press **Enter**.

6. To compile all driver modules and utilities in a multiple CPU server (SMP kernel), type the command **make** and press **Enter**

7. Are you using DM-MP for failover?

   - **Yes** – Go to step 13.

   - **No** – Go to step 8.

8. To install the RDAC failover driver, type the command **make install all** and press **Enter**.

   These actions result from running this command:

   - The driver modules are copied to the kernel module tree.

   - The new RAMdisk image (`mpp- 'uname -r'.img`) is built, which includes the RDAC driver modules and all driver modules that are needed at boot.

9. Follow the instructions at the end of the build process to add a new boot menu option that uses `/boot/mpp- 'uname -r'.img` as the initial RAMdisk image.

10. Restart the system by using the new boot menu option.

11. To make sure that RDAC is installed correctly, type the command **/sbin/lsmod** and press **Enter**.

    Make sure that these driver stacks were loaded after restart:

    - **scsi_mod**

    - sd_mod

    - **sg**

    - **mppUpper**

    - **The physical HBA driver module**

    - **mppVhba**

12. To check the RDAC version, type the command **mppUtil -V** and press **Enter**.

13. To make sure that the storage manager packages are installed correctly, type the following commands in the sequence shown, and press **Enter** after each command.

Package	Command
Runtime	rpm -q SMruntime
ESM	rpm -q SMesm
Client	rpm -q SMclient
Utilities	rpm -q SMutil
Agent	rpm -q SMagent

14. Was the installation for the selected package successful (no problems were reported)?

- **Yes** – The installation is complete.

- **No** – Repeat step 1 through step 13. If the problem persists, refer to the *Storage System Product Release Notes for Version 11.x*, or contact a Technical Support Representative.

Procedure – Installing the Storage Manager Native Packages on the Solaris OS

NOTE Before you install the client software, you must install the runtime software. Installing the storage manager packages is required for both hosts and storage management stations.

In these procedures, you must enter commands to install the applicable software packages. After each initial command, the software installation starts. When the installation has completed, a message indicates that the installation was successful. Then, you are returned to the command prompt.

1. To install the packages, type the following commands in the sequence shown, and press **Enter** after each command.

   In the table that follows, `<mount-point>` is a placeholder for the mount point for the disc, and `<SM*-package>` is a placeholder for the package name of each storage manager package.

Package	
Runtime	pkgadd -d /<mount-point>/install/native/<SMruntime-package>.pkg
ESM	pkgadd -d /<mount-point>/install/native/<SMesm-package>.pkg
Client	pkgadd -d /<mount-point>/install/native/<SMclient-package>.pkg
Utilities	pkgadd -d /<mount-point>/install/native/<SMutil-package>.pkg
Agent	pkgadd -d /<mount-point>/install/native/<SMagent-package>.pkg

2. Was the installation for the selected package successful (no problems were reported)?

- **Yes** – Go to "Restarting the System."

- **No** – Repeat step 1. If the problem persists, refer to the *Storage System Product Release Notes for Version 11.x*, or contact a Technical Support Representative.

Restarting the System

Checking the Installation on the Solaris OS

Restarting the System

NOTE If you installed RDAC, you must restart the system.

1. If the package installation choices are still on the screen, type q to exit the menu.

2. Did you install RDAC?

- **Yes** – Go to step 3.
- **No** – Go to "Checking the Installation on the Solaris OS."

3. To turn off the system, type the command `/etc/shutdown -y -i0 -g0`, and press **Enter**.

4. To restart the system, type the command `boot -r` and press **Enter**.

5. Go to "Checking the Installation on the Solaris OS."

Checking the Installation on the Solaris OS

NOTE After you have completed installing the software packages, make sure that they installed successfully.

1. At the command prompt, type the command `pkginfo -l <package-name>` and press **Enter**.

   In this command, `<package-name>` is a placeholder for the name of a package that you installed.

2. From the `/opt/StorageManager` directory, review any error messages from the error message log, and correct the problem. If the problem persists, contact a Technical Support Representative.

3. For each package that you installed, repeat step 1 through step 2.

Installing the Storage Manager Packages Using Silent Mode

You can use the Silent installation mode for any OS that is supported by Install. To install the storage manager packages using the Silent mode, locate the specified components in the installer.properties file by entering the command `SMIA.xx.xx.xx.xx.bin -f installer.properties`.

Options for Silent Installation

Custom Installation Parameters

The Default Installer.Properties File

Options for Silent Installation

The installer provides four options for Silent mode installation:

- All (client, agent, utils, failover driver)
- Custom1 (client only)
- Custom2 (host only)
- Custom

You can make the following changes to these options by changing the value of *CHOSEN_INSTALL_SET*, which is located in the *installer.properties* file.

- To install all components: *CHOSEN_INSTALL_SET=All*
- To install only the client set: *CHOSEN_INSTALL_SET=Custom1*
- To install the host configuration set: *CHOSEN_INSTALL_SET=Custom2*

- To install a customized configuration set: `CHOSEN_INSTALL_SET=Custom`

Custom Installation Parameters

These five features are available for you to install:

- SMagent
- SMutil
- RDAC
- JAVA AC

You can install one or more of the five features by entering the corresponding value. For example, to install only the SMclient and the SMutil, enter the parameter `CHOSEN_INSTALL_FEATURE_LIST=SMclient,SMutil`.

The Default Installer.Properties File

Consider the following information about the `default installer.properties` file:

- If this file is named `installer.properties` and is in the same directory as the installer, it is automatically accessed when you run the installer. If it is named something different or is in a different directory, you can enter the following **-f** option in the installer: **INSTALLER_UI=silent**

Determine which of the following install sets you want to use:

- All: SMclient, SMagent, SMutils, failover, ttsp
- Custom: Select one or more installs sets (SMclient, SMagent, SMutils, failover, ttsp)
- Custom1: SMclient only
- Custom2: SMutil, SMagent, failover

After you have determined which install set to use, enter the corresponding value. For example, to install only the SMclient enter the value `CHOSEN_INSTALL_SET=Custom1`.

If you have previously selected the Custom install set, you can choose to install only the components that you want by selecting them in the check boxes that are shown on the screen. The valid values are SMclient, SMagent, SMutil, RDAC, and Java Ac. For example, if you want to install only the SMclient, you would enter the value `CHOSEN_INSTALL_FEATURE_LIST=SMclient`.

NOTE This is the only option that allows you to select the Java Access Bridge.

You can specify whether or not to start the monitor service by entering either `0` for **Yes**, or `1` for **No**. For example, to start the monitor service, enter the following: `AUTO_START_CHOICE=0`

You can choose whether or not to reboot the system when the installation completes by entering either **Yes** or **No**. For example, if you do not want the system to reboot after the installation completes, enter the following: `USER_REQUESTED_RESTART=NO`

NOTE If the failover driver was removed during the uninstall, you will need to set the value to **NO** and manually reboot the system.

NOTE The auto-reboot does not work for the uninstall.

If a failover driver is included in the install set, you can choose which failover driver to install. If this variable is not set in a Silent installation, or if it is set to something that is not included in the bundle, an error is logged and the installation exits. The valid value is *mpio* so you would enter the following: `REQUESTED_FO_DRIVER=mpio`

Step 3 – Setting Up the Storage Array for Windows Server Core Editions

If your host is running Windows Server 2008 R2 Server Core, Windows Server 2012 Server Core, or Windows Server 2012 R2 Server Core editions, 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 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 Storage Manager Software").

4. Configure the iSCSI ports.

5. Configure and view the targets.

6. Establish a persistent login to a target.

7. Verify your iSCSI configuration.

8. Review other useful iSCSI commands.

9. Configure your storage array.

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

Server Core Setup Procedure – Configuring the Network Interfaces

Server Core Setup Procedure – Setting the iSCSI Initiator Services

Server Core Setup Procedure – Installing the Storage Management Software

Server Core Setup Procedure – Configuring the iSCSI Ports

Server Core Setup Procedure – Configuring and Viewing the Targets

Server Core Setup Procedure – Establishing a Persistent Login to a Target

Server Core Setup Procedure – Verifying Your iSCSI Configuration

Server Core Setup Procedure – Reviewing Other Useful iSCSI Commands

Server Core Setup Procedure – Configuring Your Storage Array

Server Core Setup 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.

Server Core Setup 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.

Server Core Setup Procedure – Installing the Storage Management Software

The SANtricity Storage Manager executable is located with the SANtricity Storage Manager product files, whether you download them from a Web site or install from a DVD. Refer to NetApp Support Site at support.netapp.com to find out the specific delivery method.

1. Do one of the following actions:

   - If you have been directed to a Web site, download the SANtricity Storage Manager files from the appropriate location.

   - If you are installing from a DVD, 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:\ProgramFiles \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.

Server Core Setup 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 10.86* PDF 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 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.

Server Core Setup 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 3.

   - If no, go to 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 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 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.

Server Core Setup 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.

Server Core Setup 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.

Server Core Setup 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.*

Server Core Setup 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. Refer to NetApp Interoperability Matrix at support.netapp.com/matrix 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 steps in "Procedure - Configuring the Storage" on 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* PDF for information that will help you configure your storage array.

Step 4 – Configuring the Host Bus Adapters

A host bus adapter (HBA) is an adapter on the communications 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.

You must set up the operating system (OS) type in SANtricity, using Storage Partition Mapping to configure the system to operate with the OS and Multipath driver that is installed on the host. In addition, other operating OS and failover driver settings may be necessary to make sure that your storage array runs properly. For details, refer to Step 16 – Defining the Hosts.

Refer to NetApp Interoperability Matrix at support.netapp.com/matrix 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 was new with SANtricity Version 10.83. ALUA is a feature of the controllers that provides access to a volume through any controller port.

Step 5 – Starting SANtricity Storage Manager

This topic describes starting SANtricity Storage Manager and the provides brief descriptions of the tasks performed from the Enterprise Management Window and the Array Management Window.

For Additional Information

Procedure – Starting SANtricity Storage Manager

Things to Know – Enterprise Management Window and Array Management Window

Things to Know – Icon Redesign in SANtricity Storage Manager Software

For Additional Information

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

- The *SANtricity Storage Manager Concepts Guide for Version 11.10* PDF.
- Online help topics in the Enterprise Management Window and the Array Management Window in SANtricity Storage Manager.

Procedure – Starting SANtricity Storage Manager

1. At the prompt, type SMclient, and press Enter.

2. Do the storage arrays appear in the Enterprise Management Window?

   - **Yes** – You are finished with this procedure.

   - **No** – A dialog asks whether to add the storage arrays automatically or manually. For the steps to add the storage arrays, see "Step 7– Adding the Storage Array."

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

Things to Know – Enterprise Management Window and Array Management Window

Table 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 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 (through either AutoSupport messages or email and SNMP), and perform other high-level configuration functions.
	It provides a high-level status of the health of each storage array and a summary status of all of the storage arrays, including the partially managed storage arrays, in your management domain.
	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).
Enterprise Management Window **Setup** Tab and Array Management Window **Setup** Tab	When you first start the Enterprise 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.
	When you first start the Array Management Window, the **Summary** tab is selected by default.

Figure 4. Enterprise Management Window with the Setup Tab Selected
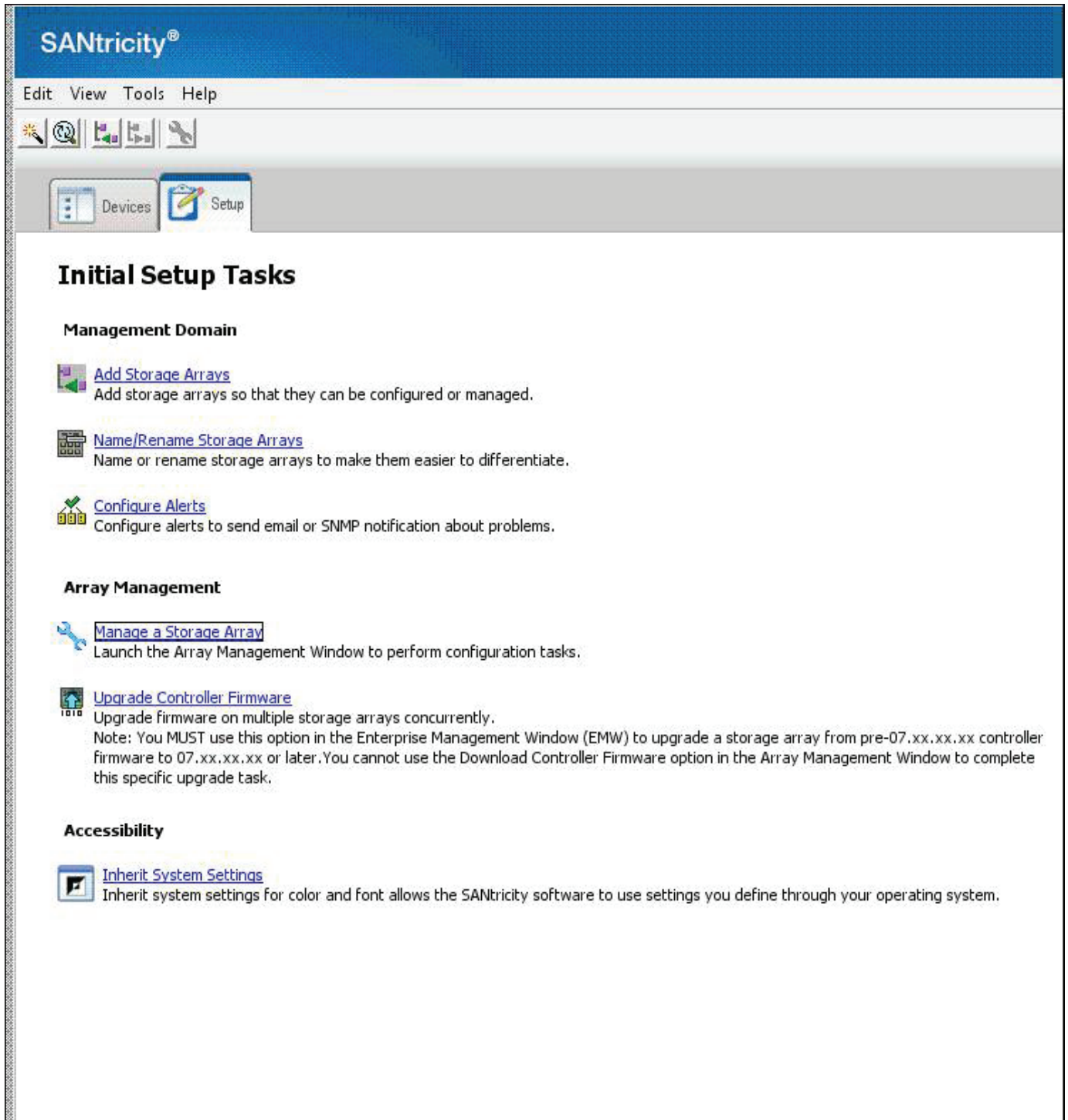
82009-01

Figure 5. Array Management Window with the Setup Tab Selected

Array Name - SANtricity® (Array Management)

SANtricity®

Storage Array   Storage   Host Mappings   Hardware   Monitor   Upgrade   Help

Array Name

Summary | Performance | 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.

Create Storage
Provision drives into appropriate storage elements.

Save Configuration
Save configuration parameters in a file to replicate the configuration on another storage array.

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.

82009-00

NOTE Both the Configure iSCSI Host Ports and the Manage iSCSI sessions appear only if your configuration is using iSCSI network protocols.

Things to Know – Icon Redesign in SANtricity Storage Manager Software

In this release, steps were taken to re-evaluate the usability of the visual aspect of the icons. The goal is to ensure that critical status indicators are more visible, visual distractions are decreased, and a more consistent pattern is applied to the status icons.

The colors green, red, and yellow are reserved for status indication only. This is most notably seen in the change from green to blue in the base volume icons.

Figure 6. Icon Colors Reserved for Status Indicators

84010-00

Status icons in the logical tree view and a few other areas are no longer combined with the object icons. The status badges are now presented to the sides of the affected object.

Figure 7. Status Indicators (Badges) to the Side of Objects Icons

Find object in tree	
Storage Array Mohawk	
All Logical Objects	
Unconfigured Capacity	
Disk Pools	
Disk Pool 1	
Free Capacity	
Volume 1	
Volume 2	
Thin Volume	
Repository	
Volume Groups	
Volume Group 1	
Volume 3	
Snapshot Group 1	
Snapshot Volume 2	
Free Capacity	
Consistency Groups	
Consistency Group 1	
Member Volumes	

Object Type:
Volumes

Refresh...

Total Volumes: 3

Standard Volumes:

Volumes:

Name	Thin Provisioned	Status	Capacity	Accessible by
Unnamed	No	Optimal	100,004 MB	Default Group
2	No	Failed	1,000 GB	Not Applicable
1	Yes	Degraded	1,000 GB	Not Applicable

82010-00

Step 6 – Manually Configuring the Controllers

If a DHCP server is not available, use this step to learn how to manually configure the IP addresses for 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.

- 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. For directions on connecting these cables, see the "Connecting the Ethernet Cables" step in the hardware installation guide for your particular configuration.

- 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.

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

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.

NOTE If your controller-drive tray uses an iSCSI protocol, you must establish the iSCSI sessions from the host to the storage array before you can use in-band management.

To discover the storage array and to manually configure the controllers, perform the procedure in <u>Procedure –
Configuring the Controllers</u>.

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 <u>Procedure – Configuring the Management Station</u>.

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.

NOTE All 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 <u>Procedure – Configuring the Controllers</u>.
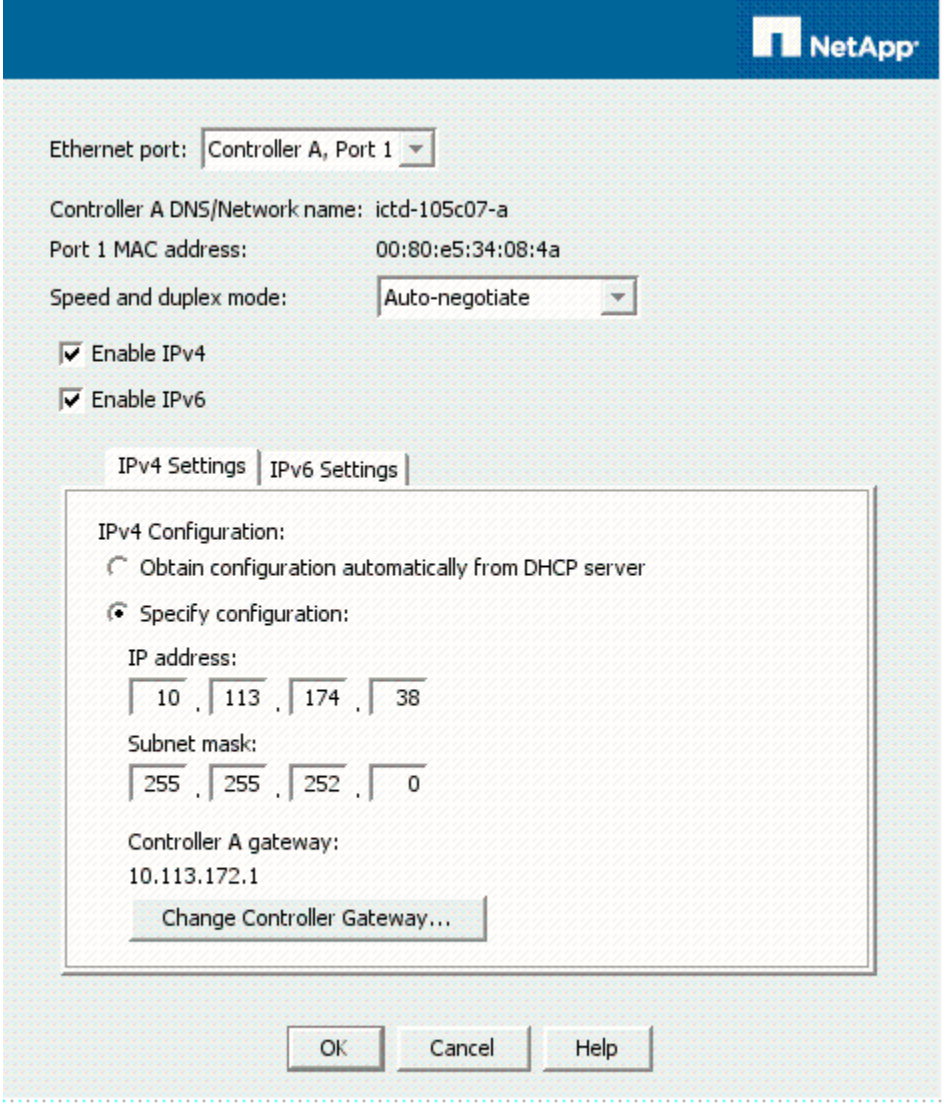
Procedure – Configuring the Controllers

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 8. Change Network Configuration Dialog with IPv4 Settings

Figure 9. Change Network Configuration Dialog with IPv6 Settings

4. Select **Controller A, Port 1** in the **Ethernet port** drop-down list.

5. From the **Speed and duplex mode** drop-down list, select **Auto-negotiate**.

   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 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

This section describes the methods for adding storage arrays to your configuration. For information about using DHCP to set up the IP address, refer to Table 1 in Things to Know – In-Band and Out-of-Band Requirements.

Things to Know – Storage Array

Procedure – Automatically Adding a Storage Array

Procedure – Manually Adding a Storage Array

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

Procedure – Rescanning the Host for a New 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 (powering on the 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 automatic discovery.

   This process finds all of the storage arrays on the local sub-network. Several minutes might elapse to complete the process.
3. Do you see the storage array in the **Devices** tab of the Enterprise Management Window?
   - **Yes** – Go to Step 8 – Naming the Storage Array.
   - **No** – Go to Procedure – Manually Adding a Storage Array (the storage array might reside outside the local sub-network).

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

Procedure – Manually Adding a Storage Array

1. From the Enterprise Management Window, click on the **Setup** tab and then click the **Add Storage Arrays** link.

   The **Select Addition Method** dialog appears. By default, the **Automatic** radio button is selected.
2. Select the **Manual** radio button and click **OK**.

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

Figure 10. Add New Storage Array – Manual Dialog

82007-00

3. 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.

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 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.

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. For instructions, refer to "Starting or Restarting the Host Agent Software" in the online help.

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

This topic describes the conventions and procedures for naming a 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:
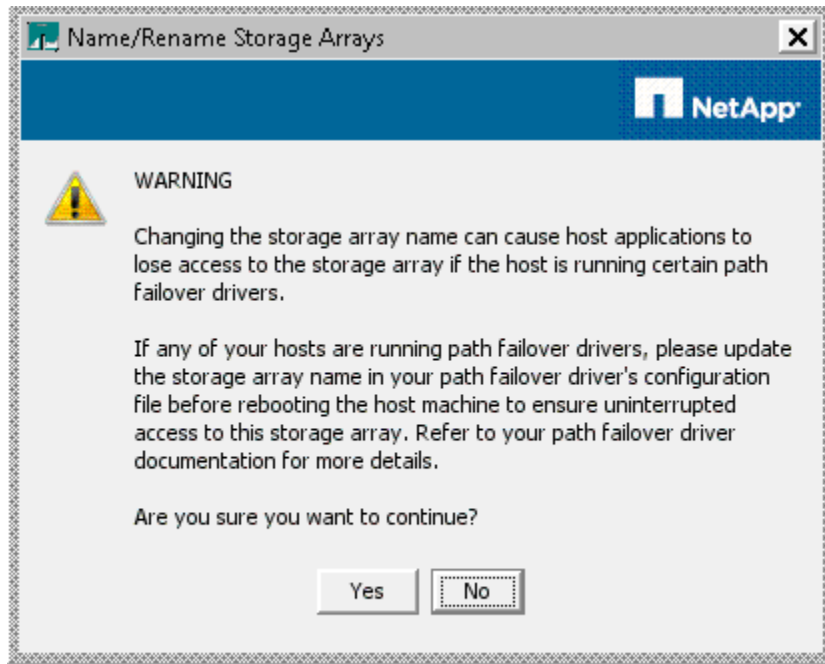
82007-02

8. Perform one of these actions:

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

- **The host is running a path failover driver** – Click **No**. Go to step 9.

9. Decide whether you have to name other storage arrays in your configuration.

- **Yes** – Click **Apply** to make the change and to keep the dialog open. Go to step 3.

- **No** – Click **OK** to make the change and to close the dialog.

10. From the **Name/Rename** dialog.

- Select another storage array to name.

- Click **Cancel** 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

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 Step 10 – Adding Controller Information for the Partially Managed Storage Array.

   - **Needs Attention** – Go to step 5.

   - **Unresponsive** – Refer to the online help topics in the Enterprise Management Window for the procedure.

5. Select **Storage Array**, and click **Recovery Guru** to launch the Recovery Guru. Follow the steps in the Recovery Guru to resolve the problem.

Step 10 – Adding Controller Information for the Partially Managed Storage Array

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

Key Terms

Things to Know – Partially Managed Storage Arrays

Procedure – Automatically Adding a Partially Managed Storage Array

Key Terms

partially managed storage array

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 44 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.

Step 11 – Setting a Password

This topic describes how to set the passwords available on your storage array.

Things to Know – Passwords

- You can configure each storage array with an Administrator password and a Monitor password.

  - Setting an Administrator password for your storage array protects it from being modified by unauthorized users. Modifying commands includes any functions that change the state of the storage array, such as creating volumes and modifying the cache settings.

  - Setting a Monitor password allows users, who are not allowed to modify storage array configurations, to view storage array configurations and to monitor storage array health conditions.

- 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.

- 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 Only a user with the Administrator password can set or change the Monitor password. If a user with View-only access (Monitor Password) attempts to launch the Set Password dialog, the system prompts for the Administrator password.

NOTE Both the Administrator storage array password and the Monitor storage array password are 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 Array Management Window, select **Storage Array >> Security >> Set Password**.

2. From the User type drop-down list, choose which password you want to set or change (either the Administrator or the Monitor password.

   If passwords are set on the storage array, the system prompts you for an Administrator password. If no passwords are set on the storage array, the User type drop-down list is disabled and the Administrator password is selected by default.

3. Complete one of the following actions:

   - If you are setting the password for the first time, type the new password in the Enter password text box and then type the new password in the Confirm password text box.

- If you are changing the Administrator password, type the new password in the New password text box and the Confirm password text box. Click **Apply**.

- If you are changing the Monitor password, type the new password in the New password text box and the Confirm password text box. Click **Apply**.

Step 12 – Removing a Storage Array

This topic describes how to remove a storage array from the Enterprise Management Window of your storage management station.

Things to Know – Removing Storage Arrays

Procedure – 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 selected 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 Storage Manager sends critical issues with the storage array to the correct email address.

Key Terms

Things to Know – AutoSupport (ASUP) Messages

Procedure – Configuring the Delivery Method for AutoSupport Messages

Things to Know – Alert Notifications Using Email or SNMP Traps

Procedure – Setting Alert Notifications

Key Terms

Management Information Base (MIB)

Simple Network Management Protocol (SNMP)

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 – AutoSupport (ASUP) Messages

The AutoSupport (ASUP) feature collects data in a customer support bundle from all AutoSupport-enabled storage arrays and automatically sends the data to Technical Support for remote troubleshooting and problem analysis with the storage management software. All of the data is compressed into a single compressed archive file format (7z) at the location you specify.

Two methods of collecting support data exist in the storage array: the AutoSupport feature and the Legacy Collect Support Data feature. With AutoSupport, data is automatically sent to Technical Support instead of manually sending it to Technical Support, as is done with Legacy Collect Support Data feature. The AutoSupport implementation speeds up troubleshooting and problem analysis.

The AutoSupport feature is the preferred data collection method to use if available on your storage array.

AutoSupport messages include three types:

- Event messages
    - Sent when a support event on the managed storage array occurs
    - Includes system configuration and diagnostic information
- Daily messages
    - Sent once every day during a user configurable time interval, local time of the storage array
    - Includes the current system event logs and performance data
- Weekly messages
    - Sent once every week during a user configurable time interval, local time of the storage array
    - Includes configuration and system state information

Before you configure the AutoSupport feature, make sure the following conditions are true:

- The AutoSupport feature must be enabled and activated on the storage array. (The AutoSupport feature is activated and de-activated globally on a storage management station and may be enabled or disabled for an individual storage array.)
- The Storage Manager Event Monitor must be running on at least one machine with access to the storage array and, preferably, on no more than one machine.

Procedure – Configuring the Delivery Method for AutoSupport Messages

1. From the **Devices** tab on the Enterprise Management Window, click **Discovered Storage Arrays**, and then select **Tools >>AutoSupport >>Configuration**.
   The **AutoSupport Configuration** dialog appears.

2. Select the message delivery method by clicking one of the following radio buttons.
    - **HTTPS** allows you to connect directly to the destination technical support system using the HTTPS protocol as the AutoSupport delivery method.
    - **HTTP** allows you to connect directly to the destination technical support system using the HTTP protocol as the AutoSupport delivery method.
    - **Mail (SMTP) Server** allows you to designate where alert emails are sent, such as to the destination technical support system.

3. Do one of the following:
    - If you selected either HTTPS or HTTP, go to step 4.
    - If you selected SMTP, go to step 5.

4. If you selected either the HTTPS or the HTTP mail delivery method, select one of the following delivery parameters:
    - **Direct** is the default selection that allows you to connect directly to the destination technical support system using the HTTPS or HTTP protocol.
    - **Proxy Server** allows you to specify the HTTP proxy server details required for establishing connection with the destination technical support system. You must specify the host address and port number.; however, you need only enter the host authentication details (user name and password) if required.
    - **Automatic Proxy Configuration Script (PAC)** that specifies the location of a PAC file that allows the system to automatically choose the appropriate proxy server for establishing a connection with the destination technical support system.

5. If you selected mail (SMTP) server, specify the name of the mail server and the sender's email address required for sending an email to the destination technical support system and the Reply-to email address required for sending a sample AutoSupport message.

6. Click **Send Sample ASUP message** to test the connection to the destination technical support system using the specified mail delivery parameters.

    -   If the configuration test succeeds, the system shows the **AutoSupport Message Send Successful** dialog. Click **OK** to dismiss the error dialog.

    -   If the configuration test fails, the system shows the **AutoSupport Message Send Failed** dialog. Click **OK** to dismiss the error dialog.

7. Click **OK** to save the message delivery parameters.

Things to Know – Alert Notifications Using Email or SNMP Traps

Setting alert destinations lets you specify addresses for the delivery of email messages and SNMP trap messages whenever a critical problem occurs with the storage array. For more specific notifications, you can configure the alert destinations at the storage management station, host, and storage array levels.

-   To set up alert notifications using SNMP traps, you must copy and compile a management information base (MIB) file on the designated network management stations. The MIB file might be part of the storage management software package, or separately available in the download area where you obtained the management software.

-   To send email to alert destinations, you must specify a mail server and a sender email address.

-   To decode and show SNMP traps sent by the storage management software, you can configure a host running a network management station to perform these tasks. You must copy and compile a management information base (MIB) file on the designated network management stations.

-   You must have Event Monitor running on a machine (a management station or a host) to receive alerts. The machine should be one that runs continuously.

NOTE If you choose not to automatically enable the event monitor during installation, you do not receive critical alert notifications. However, you can start Event Monitor later, assuming Event Monitor is installed on at least one machine with access to the array. Note that Event Monitor must be running and that alert settings must already be configured at the time of an alertable event, otherwise, there will be no alert for that event because alerts were not enabled at the time of that event.

Procedure – Setting Alert Notifications

1. From the **Devices** tab on the Enterprise Management Window, select a node and click **Edit >> Configure Alerts**. The **Configure Alerts** dialog appears.

2. Select one of the following radio buttons an alert level:

    -   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.

    These results occur, depending on your selections:

    -   If you selected the **All storage arrays** radio button, the **Configure Alerts** dialog appears.

    -   If you selected the **An individual storage array** radio button, the **Select Storage Array** dialog appears. Select the storage array for which you want to send email alerts, and click **OK**. The **Configure Alerts** dialog appears.

> **NOTE** If you do not know which storage array to select, click **Locate** to turn on the LEDs of the storage array.

3. Perform one of these actions:

    - To configure email alert destinations– Go to step 4.

    - To configure SNMP alert destinations – Go to step 11.

4. In the **Configure Alerts** dialog, select the **Mail Server** tab.

5. In the **Mail server** text box, type the name of the Simple Mail Transfer Protocol (SMTP) mail server.

    The SMTP mail server is the name of the mail server that forwards the alert emails to the configured email addresses.

6. In the **Email sender address** text box, type the email sender address. Use a valid email address.

    The email sender address is the email address of the sender that appears on each email alert sent to the destination. The email sender address is usually the address for the network administrator.

    > **NOTE** To include the contact information of the sender in the email alert, select the **Include contact information with the alerts** check box, and type the contact information in the text box. Including the contact information in the email alert is optional.

7. Select the **Email** tab to configure the email destinations.

    - To add an email address – In the **Email address** text box, type the address, and click **Add**.

    - To replace an email address – In the Configured email addresses area, select the email address to be replaced, type the replacement address in the **Email address** text box, and click **Replace.**

    - To delete an email address – In the Configured email addresses area, select the email address, and click **Delete**.

    - To validate an email address – Either type the email address in the **Email address** text box or select the email address in the Configured email addresses area, and click **Test**. A test message is sent to the selected email address. A dialog appears with the results of the validation and any errors.

8. In the **Information To Send** drop-down list, select one of the following options:

    - **Event Only** – The alert email contains only the event information. This alert type is the default.

    - **Event + Profile** – The alert email contains both the event information and the profile information.

    - **Event + Support** – The alert email contains the event information and a compressed file that contains complete support information for the storage array that has generated the alert.

9. In the **Frequency** drop-down list, select one of the following options:

    - **Every event** sends an alert email whenever an alertable event occurs. This option is the default.

    - **Every x hours** sends an alert email after the specified time interval if an event occurred during that time interval. You can select this option only if you have selected either **Event + Profile** or **Event + Support** in the **Information To Send** drop-down list.

    Keep the following guidelines in mind:

    - You must provide an SMTP mail server name and an email sender address for the email addresses to work.

    - The email addresses that you had previously configured appear in the Configured email addresses area.

    - You must use fully qualified email addresses, for example, *name@mycompany.com*.

    - You can configure multiple SNMP addresses before you click **OK**.

10. Click **OK**.

    An alert icon appears next to each node in the Tree view where an alert is set. You are finished with this procedure.

11. In the **Configure Alerts** dialog, select the **SNMP** tab.

- To add an SNMP address, in the Community name text box, type the community name. In the Trap destination text box, type the trap destination, and click **Add**.

> **NOTE** The community name is an American Standard Code for Information Interchange (ASCII) string that identifies a known set of network management stations and is set by the network administrator. The default community name is public. The trap destination is the IP address or the host name of a computer running an SNMP service. At a minimum, the trap destination is the network management station.

- To replace an SNMP address, select the SNMP address in the Configured SNMP addresses area, type the replacement community name in the Community name text box and the trap destination in the Trap destination text box, and click **Replace**.
- To delete an SNMP address, select the SNMP address in the Configured SNMP addresses area, and click **Delete**.
- To validate an SNMP address, select the SNMP address in the Configured SNMP addresses area, and click **Test**. A test message is sent to the SNMP address. A dialog appears with the results of the validation and any errors.

Keep this information in mind:

- Any SNMP addresses that you had previously configured appear in the Configured SNMP addresses area.
- The SNMP Community Name is set in the configuration file of the network management station by a network administrator.
- You can configure multiple SNMP addresses before you click **OK**.

12. Click **OK**.

An alert icon appears next to each node in the Tree view for which an alert is set.

Step 14 – Changing the Cache Memory Settings

This topic describes how you can modify cache memory settings in your storage array through the SANtricity Storage Manager to enhance system performance.

NOTE Cache settings are performed at two levels: block size and flushing for the entire storage array and volume level settings. The storage array level settings can be configured at this step; however, the volume level settings cannot be configured until volume groups and volumes have been created. For information about creating volume groups and volumes, refer to .

Key Terms

Things to Know – Cache Memory Settings

Procedure – Viewing the Cache Memory Size Information

Procedure – Changing the Storage Array Cache Settings

Procedure – Changing the Volume Cache Memory Settings

Key Terms

cache memory

cache memory

An area of random access memory (RAM) on the controller. This memory is dedicated to collecting and holding related data until a drive tray or a 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

- Cache memory settings can be configured at the storage array and individual volume levels to optimize performance for your application.
- When read caching is enabled on a volume, a check is performed to determine if data requested from a host read operation is available in cache memory. If so, the requested data is read from the cache memory and no drive access is required. Read caching improves read performance for most workloads. Dynamic cache read prefetch can be enabled to further improve read performance for sequential read operations, such as multimedia.
- When write caching is enabled for a volume, write data is written initially to the controller's cache memory. When a percentage of unwritten data is reached, the data is flushed from cache memory and written to the drives. 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 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.

- 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. Cache mirroring should always be enabled so that unwritten data in the cache will be preserved if a controller failure occurs.

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 **Base Controller Properties** view appears in the right pane.

5. Scroll through the **Base Controller Properties** tab until you find the cache information and the cache backup device information. Note that a portion of the controller's cache memory is used as processor cache and the remainder is used as data cache for host read and write operations.

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 cache memory to trigger a cache flush in the **Start demand cache flushing** text box.

5. Select the desired 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.

a. 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.

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

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**. Multiple volumes can be selected by using the `Control` or `Shift` keys or the **Select all** check box.

Step 15 – Enabling the Premium Features

This topic describes how you can enable premium features that are available with SANtricity Storage Manager.

NOTE If you did not obtain any premium feature key files at NetApp Support Site at support.netapp.com, skip this step.

Key Terms

Things to Know – Premium Features

Procedure – Enabling the Premium Features

Key Terms

premium feature

premium feature

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

Things to Know – Premium Features

You enable a premium feature through a feature key file that you obtain from NetApp Support Site at support.netapp.com. The premium feature is either enabled or disabled.

Use the following procedure to obtain any of the premium features available with SANtricity Storage Manager.

Procedure – Enabling the Premium Features

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

The **Premium Features installed on storage array** drop-down list shows the name and the status of the premium feature that you have enabled.

8. Repeat step 4 through step 7 for each premium feature that you want to enable.

Step 16 – Defining the Hosts

NOTE If you will not use storage partitions or you do not have the SANshare Storage Partitioning 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 or Procedure – Defining the iSCSI Hosts.

NOTE You must know the unique initiator port name of each HBA port (World Wide Port Names in the case of FC). If you have not already recorded them, see the "Installing Host Bus Adapters" topic in the installation guide for your particular configuration (E2600 controller-drive tray, E2660 controller-drive tray, E5400 controller-drive trays, or E5500 controller-drive trays) for instructions to obtain these unique initiator port names.

Key Terms

Things to Know – Hosts

Things to Know – Host Groups

Things to Know – Storage Partitions

Procedure – Defining the Hosts

Procedure – Defining the iSCSI Hosts

Key Terms

host context agent

host context agent

A software component that runs on each of the hosts in a storage area network (SAN). The host context agent collects SAN topology information from the host and sends the information to each storage array that is attached to the host. The host context agent collects the host name, the host type, and the unique initiator port name for each HBA host or, in the case of FC, the World Wide Identifier (WWID) for each HBA host port. The host context agent is not available on all supported OSes. If it is not available, the hosts can be defined manually.

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 services 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 If your operating system configures automatically, then, by default, the host context agent automatically defines all attached hosts that are running SMagent in the mapping view of the AMW with a default mapping 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.

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 feature that was either already enabled on your storage array at the factory, or you must purchase a feature key file to enable it. Refer to NetApp Support Site at support.netapp.com for information about obtaining a feature key file.

- You do not create storage partitions in this step, but you must understand them to define your hosts.

- Even if you do not use storage partitions, you must select the Host Operating System type for the Default Group.

- You *do not* need to create storage partitions if these conditions exist (see Figure "Example of No Additional Storage Partitions Required"):

  - 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 within a storage partition, whether it is the Default Partition or one that you create, must have the same operating system (homogeneous). When you have multiple hosts accessing the volumes in a storage partition, 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 "Additonal Storage Partitions Required").

- You *do* need to create storage partitions if these conditions exist:

  - You want certain hosts to access only certain volumes (see "Example of Additional Storage Partitions Required (Homogeneous Host)."

  - 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 "Example of Additional Storage Partitions Required (Heterogeneous Hosts)."

Figure 11. Example of No Additional Storage Partitions Required

77039-10

Host 1

Windows Server
2012 OS

Default
Group
(Partition)

Volume 1
Volume 2
Volume 3
.
.
.
Volume N

Host 1 accesses
all volumes
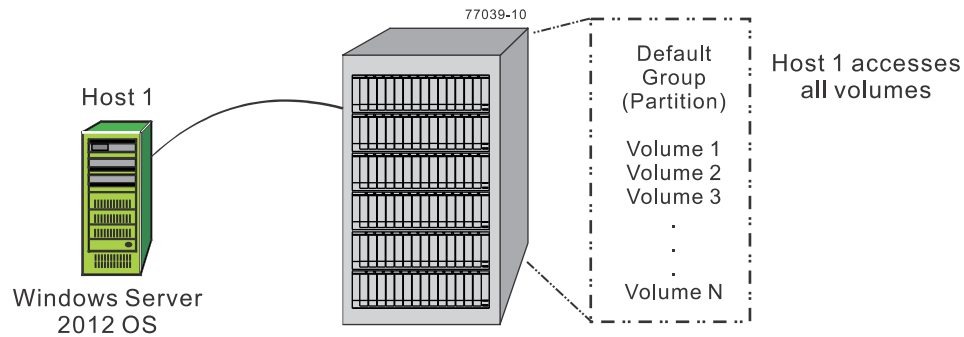
A single host accesses **all** volumes;
no additional storage partitions are needed.

Host 1

Host 2

Windows
Server
2012 OS

Windows
Server
2012 OS

Default
Group
(Partition)

Volume 1
Volume 2
Volume 3
.
.
.
Volume N

Host 1 and 2
access all
volumes
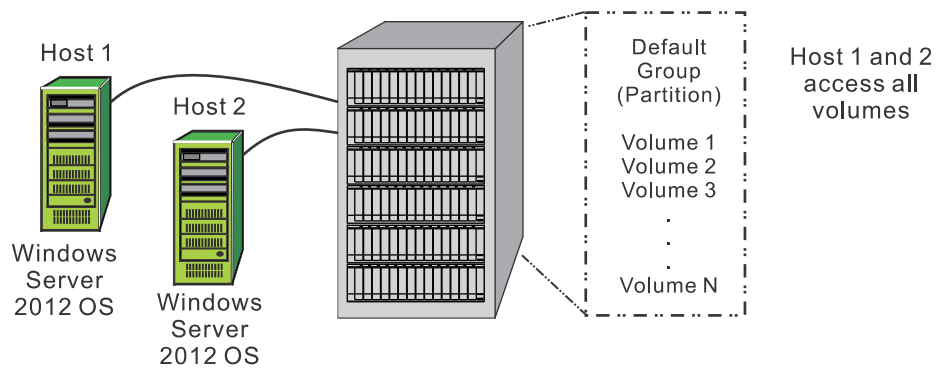
Multiple homogeneous hosts share access to **all** volumes;
no additional storage partitions are needed and
no specific host group is needed.

Figure 12. Example of Additional Storage Partitions Required (Homogeneous Host)
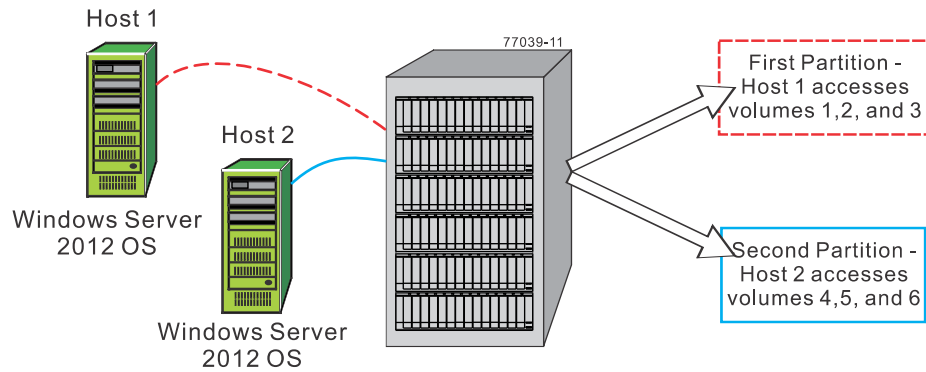
- Each host needs access to specific volumes.
- Both hosts use the same operating system (homogeneous).
- Storage divided into two logical storage partitions.
- A Default Group (partition) is not used.

Figure 13. Example of Additional Storage Partitions Required (Heterogeneous Hosts)
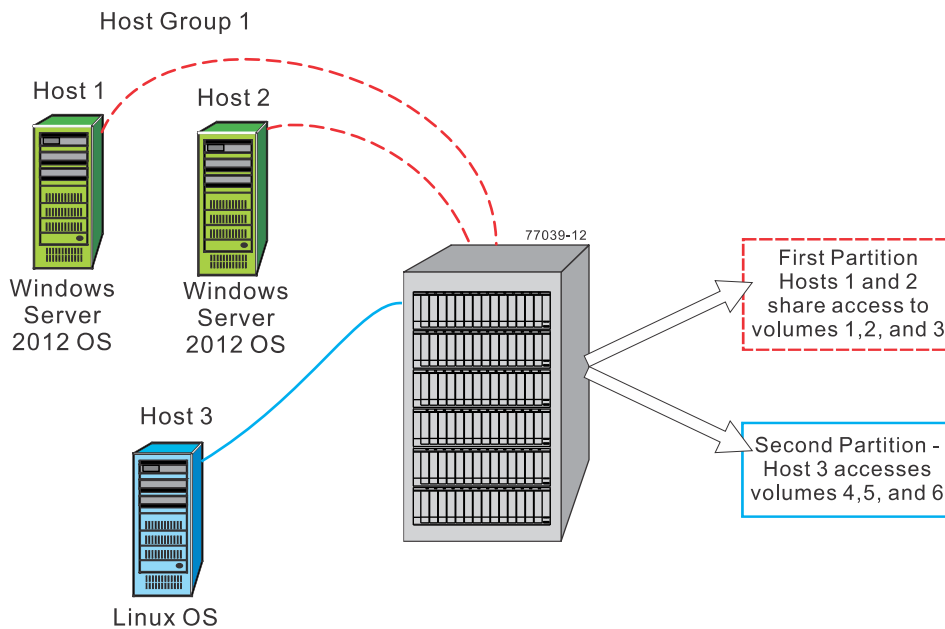
- Host 1 and host 2 (Windows Server 2012 OS) share access to specific volumes through host group 1.

- Two heterogeneous hosts (Linux OS and Windows Server 2012 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. Make sure you confirm or set the Default Operating System for your host or hosts even if you are using Default Group to ensure proper settings for failover.

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.

Key Terms

Things to Know – Data Assurance

Things to Know – Allocating Capacity

Things to Know – Disk Pools and Disk Pool Volumes

Things to Know – Volume Groups and Volumes

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

Things to Know – Hot Spare Drives

Things to Know – Full Disk Encryption

Procedure – Configuring the Storage

Key Terms

Default Group

disk pool

free capacity

full disk encryption (FDE)

hot spare drive

Redundant Array of Independent Disks (RAID)

storage partition

unconfigured capacity

volume

volume group

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.

disk pool

A set of drives that is logically grouped. A disk pool provides the overall capacity needed to create one or more volumes. A disk pool is similar to a volume group, with the following differences. The data in a disk pool is stored randomly on all of the drives in the disk pool, unlike data in avolume group which is stored on the same set of drives. You do not specify a RAID level for a disk pool. A disk pool does not use hot spare drives. A disk pool allows a large number of drives to be grouped.

free capacity

Unassigned space in a volume group or disk pool that can be used to create volumes.

full disk encryption (FDE)

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

hot spare drive

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 reconstruction of user data in the event that one, or two for RAID 6 and Dynamic Disk Pools, 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 within 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 – Data Assurance

The Data Assurance (DA) 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 feature. When you install the DA feature on a storage array, SANtricity Storage Manager provides options to use DA with certain operations. For example, you can create a volume group or disk pool that includes DA-capable drives, and then create a volume within that volume group or disk pool that is DA-enabled. Other operations that use a DA-enabled volume have options to support the DA feature.

If you choose to create a DA-capable volume group or disk pool, 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 feature is enabled, the **DA Enabled** check box appears in the **Create volume** dialog box under **Quality of Service Attributes**. 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. If you choose to enable DA, it must be enabled at the time of volume creation as it cannot be enabled later after volume initialization has completed.

When the DA 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.

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 – 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 logical entities, known as volume groups, disk pools, and volumes.

Volume groups and disk pools are sets 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 unconfigured 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
  - Increasing the free capacity of a volume group or disk pool to add new volumes
  - 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.

- Mixing drives with different media types or interface types within one volume group or disk pool is not permitted. For example, 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.

- If you are adding capacity to a Drive Security 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 have the option to enable Drive Security on newly created volumes within the volume group or disk pool.

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 across a set of drives that have been algorithmically selected from the disk pool. The data for any volume in a disk pool is distributed across all drives in the disk pool, unless the volume is very small. 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, simply select the drives from a list of eligible drive candidates. After a disk pool is created, you create volumes.

- **Better Utilization of Drives** – 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.

- **Improved Reconstruction Experience** – Disk pools do not use hot spare drives for data protection like a volume group does. Instead, spare capacity is allocated within each drive that comprises the disk pool, thus distributing the reconstruction workload. This means that reconstruction of failed drives completes faster and has less impact on performance than traditional volume group reconstruction.
- **Reduced Administration** – 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 because the spare capacity is distributed within the disk pool.

For more information about Disk Pools, refer to *SANtricity Storage Manager Concepts* guide and the online help in *SANtricity Storage Manager*.

Things to Know – Volume Groups and Volumes

- You can create a single volume or multiple volumes per volume group. You can 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.

- While creating volume groups, you should 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.
- If your drive trays or controller-drive trays have multiple drawers within them, make sure that the drives that comprise the volume group are located in different drawers within each drive tray.
- 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 automatically enabled 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.

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). Make sure to set the Default Host Operating System.

- **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. Make sure 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 hot spare drive must be the same drive type and have a capacity that is equal to or larger than the particular failed drive in order to spare for the failed drive.

Things to Know – Full Disk Encryption

Drive Security is a feature that prevents 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 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 secure the drives in a security-capable volume group or disk pool, 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 a non-FDE drive until it is security enabled.

Security-enabled drives transition to a *security-locked* state when the controller-drive tray is powered off or if a drive is removed from the drive tray. 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 or non-capable

- Secure – Security enabled or disabled

- Read/Write Accessible – Security locked or unlocked

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

- Security-capable
- Secure

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

Table 8. 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 feature has been enabled, the **Drive Security** menu appears in the **Storage Array** menu under **Security**. The **Drive Security** menu has these options:

- **Create Key**
- **Change Key**
- **Import Key**
- **Save Key**
- **Unlock Drives**
- **Validate Key**

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

If you have created a security key for the storage array, the **Create Key** option is inactive with a check mark to the left. The **Change Key** option, the **Save Key** option, and the **Validate 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 volume group or disk pool selected in the **Storage & Copy Services** tab is not security enabled but is composed entirely of security-capable drives.
- The volume group contains no snapshot (legacy) base volumes or snapshot (legacy) repository volumes.
- The volume group is in Optimal state.
- A security key is set up for the storage array.

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

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

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

NOTE 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: **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.

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

   - **A storage partition is required** – Go to step 7.

6. Perform these actions:

   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 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 59.

Appendix A: 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.

NOTE If you are using the in-band management method and generate large amounts of network traffic on the same host/server connection, in-band management operations could time out because I/O and the in-band management operations are competing for the same resources.

If you receive a message about a controller operation failing because of a communication error, a time out, or an internal error with the return code 582, try the following actions to resolve the issue:

1. Verify that the physical connection used for in-band management is active and free of any sort of transmission or link type errors, and then retry the command.
2. Reduce the I/O traffic on the physical server connections being used by in-band management.
3. Try using out-of-band management.

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**.

Appendix B: Boot Device Installation

Use these procedures if you are setting up the storage array as a boot device.

Boot Device Support

Installing the Boot Device

Boot Device Support

Not all operating systems support the use of a storage array as a boot device. Support for using a boot device also depends on the type of host connection. Fibre channel and SAS connections are supported. InfiniBand and iSCSI connections are not supported. The following table shows which operating systems support this configuration.

Table 9. Operating System Support for Using a Storage Array as a Boot Device

Operating System	Boot Device Support
Windows Server 2012 Windows Server 2008 R2 Hyper-V	Yes, where supported by the HBAs
Solaris	Yes, where supported by the HBAs
RHEL	Yes, where supported by the HBAs
VMware	Yes, where supported by the HBAs
Mac OS X	No
AIX	Yes, where supported by the HBAs

Installing the Boot Device

This section contains procedures to install a boot device on a storage array.

Before you install the storage management software components on the host, you must prepare the storage array and the host.

ATTENTION Possible loss of data access – When you use boot device on a storage array, make sure that you have redundant connections with failover protection between the host and the storage array. Refer to the Host Cabling chapter in the Hardware Cabling Guide for information about such connections.

You must have administrator privileges to access this software. You must use the volume mapped to LUN 0 as the boot device. Some operating systems support booting only from LUN 0.

General Preparation

Preparing the Storage Array as a Boot Device

Preparing the Host

General Preparation

To prepare the storage array as a boot device, perform these procedures in order:

1. Perform the instructions in "Preparing the Storage Array as a Boot Device."

2. Perform the instructions in "Preparing the Host."

Before you proceed with the installation, confirm the following items:

- Make sure that you have access to a storage management station for the storage array. The storage management station is a host with SMclient software installed, and is not the host that you will configure to use the boot device.

- Make sure that you know the Internet Protocol (IP) addresses or host names of the controllers in the storage array from which you want to boot.

- If you have questions or concerns about the installation procedures, contact your Technical Support Representative.

Preparing the Storage Array as a Boot Device

Perform the following tasks in the order in which they appear.

Starting the SMclient Software

Configuring the Boot Volume on the Storage Array

Configuring the Boot Volume on an Unconfigured Capacity Node

Configuring the Boot Volume on a Free Capacity Node

Ensuring a Single Path to the Storage Array

Starting the SMclient Software

1. On the management station (the external host with SMclient software installed), start the existing storage management software with the procedure for your operating system:

   - **UNIX-based operating systems** – At the prompt, type `SMclient`, and press **Enter**.

   - **Windows operating systems** – Select **Start** > **Programs** > **SANtricity Storage Manager SMclient**.

   After the client software starts, the Enterprise Management Window and the Select Addition Method dialogs appear:

2. To close the **Select Addition Method** dialog, click **Cancel**.

3. Select **Edit** > **Add Storage Array**.

   The **Add New Storage Array** dialog appears.

4. Add the Internet Protocol (IP) addresses or host names of the controllers in the storage array.

   You must add the IP addresses or host names of the controllers one at a time. For more information, refer to the online help topics in the Enterprise Management Window.

   The storage array that you plan to use as the boot device appears in the Enterprise Management Window.

5. Go to "Configuring the Boot Volume on the Storage Array."

Configuring the Boot Volume on the Storage Array

1. In the Enterprise Management Window, select the storage array in the Device Tree.

2. Select **Tools** > **Manage Storage Array**.

   The Array Management Window for the selected storage array appears.

3. Select the **Storage & Copy Services** tab.

4. To determine where you can create a boot volume for the host, examine the Free Capacity nodes and Unconfigured Capacity nodes on the storage array.

   Do you have 2 GB of capacity on either the Unconfigured Capacity node or a Free Capacity node?

   - **Yes** – Go to step 5.

   - **No** – You need to free enough capacity for the boot volume. Refer to "SANtricity Storage Manager Concepts" guide or the SANtricity online help for information about freeing capacity. Add the required capacity before you continue with step 5.

5. Decide which type of capacity you will use:

   - **Unconfigured Capacity node** – Go to "Configuring the Boot Volume on an Unconfigured Capacity Node."

   - **Free Capacity node** – Go to "Configuring the Boot Volume on a Free Capacity Node."

Configuring the Boot Volume on an Unconfigured Capacity Node

1. Right-click the Unconfigured Capacity node, and click **Create Volume**.

   The **Default Host Type** dialog appears.

2. Select the default host type from the list, and click **OK**.

   The **Create Volume Wizard Introduction** dialog appears.

3. Click **Next**.

4. Select **Unconfigured Capacity** (create new volume group), and click **Next**.

   The **Specify Volume Group Parameters** dialog appears.

5. Specify the RAID level and capacity that you want for the volume group.

   A two-drive, RAID Level 1 volume group is recommended. However, you can specify more drives and RAID Level 3, RAID Level 5, or RAID Level 6.

6. Click **Next**.

   The **Specify Volume Parameters** dialog appears.

7. Specify the boot volume capacity.

   A capacity of 4 GB is recommended. The capacity must be at least 2 GB.

8. Name the volume to identify it as the boot volume.

9. From the Advanced Volume Parameters area, select **Customize settings**.

10. Click **Next**.

11. In the **Specify Advanced Volume Parameters** dialog, perform these steps:

    a. From the Volume I/O characteristics area, select **File System**.

    b. From the Preferred controller ownership area, select **Slot A**.

    c. From the Volume-to-LUN Mapping area, select **Map Later with Storage Partitioning**.

12. To create the volume and the volume group, click **Finish**.

    The **Create Volume Wizard – Creation Successful** dialog appears.

13. Click **No**.

14. Click **OK**.

15. Use the Storage Partitioning feature to map the volume to the host that uses LUN 0.

> **NOTE** For additional information about how to map volumes that use Storage Partitioning, refer to the online help topics in the Array Management Window.

16. Choose one of the following options:
    - If your host supports asynchronous logical unit access (ALUA), go to "Preparing the Host."
    - If your host does not support ALUA, go to "Ensuring a Single Path to the Storage Array."

Configuring the Boot Volume on a Free Capacity Node

1. Right-click the Free Capacity node that you want to use, and click **Create Volume**.
   The **Default Host Type** dialog appears.

2. Select the default host type from the list, and click **OK**.
   The **Create Volume Wizard Introduction** dialog appears.

3. Click **Next**.
   The **Specify Volume Parameters** dialog appears.

4. Specify the boot volume capacity.
   A capacity of 4 GB is recommended. The capacity must be at least 2 GB.

5. Name the volume to identify it as the boot volume.

6. From the Advanced Volume Parameters area, select **Customize settings**.

7. Click **Next**.

8. In the **Specify Advanced Volume Parameters** dialog, perform these steps:
   a. From the Volume I/O characteristics area, select **File System**.
   b. From the Preferred controller ownership area, select **Slot A**.
   c. From the Volume-to-LUN Mapping area, select **Map Later with Storage Partitioning**.

9. To create the volume and the volume group, click **Finish**.
   The **Create Volume Wizard – Creation Successful** dialog appears with a prompt to configure another boot volume.

10. Click **No**.

11. Click **OK**.

12. Use the Storage Partitioning premium feature to map the volume to the host by using LUN 0.

> **NOTE** For additional information about how to map volumes that use Storage Partitioning, refer to the online help topics in the Array Management Window.

13. Choose one of the following options:
    - If your host supports asynchronous logical unit access (ALUA), go to "Preparing the Host."
    - If your host does not support ALUA, go to "Ensuring a Single Path to the Storage Array."

Ensuring a Single Path to the Storage Array

After you have configured a boot volume, make sure that there is a single path to the storage array. The path must be configured to the controller that owns the boot volume (controller A).

NOTE If you removed a previously installed version of RDAC in a root-boot environment, you do not need to remove the installed version of RDAC again.

1. Remove the host interface cable to the alternate path.

   ATTENTION Possible data corruption – When you start the storage array, there must be only a single path to the storage array when RDAC is removed. The path must be to the controller that owns the boot volume. If the host is permitted to start without RDAC and still has dual paths to the storage array, the data might become unusable.

2. Boot the host system.
3. Go to "Preparing the Host."

Preparing the Host

ATTENTION Possible loss of access to the boot device and the operating system – After you install the boot device, never delete the volume mapped to LUN 0 or select **Configure** > **Reset Configuration**. Performing these actions causes loss of access to the boot device and the operating system.

In this procedure, the default boot path refers to controller A, which owns the boot volume. The alternate boot path refers to controller B.

1. Enable the BIOS on the HBA that is connected to the default boot path.

   For procedures about how to enable the HBA BIOS, refer to the host system documentation and the HBA documentation. After the BIOS is enabled, the host reboots automatically.

2. Install the operating system on the host.
3. After the installation is complete, restart the operating system.

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 1:2007. 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.

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。

Copyright information

Copyright © 1994–2013 NetApp, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means— graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277