## Contents

<table>
<thead>
<tr>
<th>Deciding whether to use this guide</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deciding on the management method</td>
<td>8</td>
</tr>
<tr>
<td>Key terms</td>
<td>8</td>
</tr>
<tr>
<td>access volume</td>
<td>8</td>
</tr>
<tr>
<td>in-band management</td>
<td>8</td>
</tr>
<tr>
<td>out-of-band management</td>
<td>8</td>
</tr>
<tr>
<td>stateless address autoconfiguration</td>
<td>8</td>
</tr>
<tr>
<td>storage manager event monitor</td>
<td>8</td>
</tr>
<tr>
<td>Management methods</td>
<td>8</td>
</tr>
<tr>
<td>Out-of-band and in-band requirements</td>
<td>11</td>
</tr>
</tbody>
</table>

### Deciding which packages to install                      14

<table>
<thead>
<tr>
<th>Key terms</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>14</td>
</tr>
<tr>
<td>host</td>
<td>14</td>
</tr>
<tr>
<td>multi-path driver, failover driver</td>
<td>14</td>
</tr>
<tr>
<td>storage management software</td>
<td>14</td>
</tr>
<tr>
<td>storage management station</td>
<td>14</td>
</tr>
<tr>
<td>storage manager event monitor</td>
<td>14</td>
</tr>
<tr>
<td>Host operating systems</td>
<td>14</td>
</tr>
<tr>
<td>Storage management software components</td>
<td>15</td>
</tr>
</tbody>
</table>

### SANtricity Storage Manager installation options         19

<table>
<thead>
<tr>
<th>Minimum system requirements for SANtricity Storage Manager</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing SANtricity Storage Manager packages using silent mode</td>
<td>19</td>
</tr>
<tr>
<td>Options for silent installation</td>
<td>19</td>
</tr>
<tr>
<td>Custom installation parameters</td>
<td>20</td>
</tr>
<tr>
<td>The default installer.properties file</td>
<td>20</td>
</tr>
<tr>
<td>AIX and VIOS: Installing E-Series entries in the ODM</td>
<td>21</td>
</tr>
<tr>
<td>Uninstalling previous E-Series entries</td>
<td>21</td>
</tr>
<tr>
<td>Installing new E-Series entries</td>
<td>22</td>
</tr>
<tr>
<td>Validating the ODM in AIX and VIOS</td>
<td>23</td>
</tr>
<tr>
<td>Windows Server Core: Installing SANtricity Storage Manager</td>
<td>24</td>
</tr>
<tr>
<td>Solaris: Configuring the host bus adapters</td>
<td>25</td>
</tr>
</tbody>
</table>

### Preparing to add the storage array to the management domain 26

| Completing preliminary tasks for preparing the storage array | 26 |
| Setting IP addresses                                        | 26 |
| Naming the storage array                                    | 27 |

### Adding the storage array to the management domain        28

| Choosing the method for adding the storage array to the management domain | 28 |
| Using automatic discovery: Out-of-band management              | 29 |
| Using DHCP and then changing to static addressing              | 30 |
| Manually adding a storage array: Out-of-band management        | 31 |
Configuring DHCP addressing .......................................................... 32
Adding the storage array for in-band management .......................... 33
Manually configuring the controllers by using the in-band method initially .......... 34
Manually configuring the controllers by setting up a temporary private network .... 36
Using the Service Interface to set IPs .................................................... 38

**Configuring other SANtricity options** ................................................ 41
Enterprise Management Window and Array Management Window .......... 41
AutoSupport (ASUP) messages ......................................................... 43
Alert notifications using email or SNMP traps ..................................... 44
Passwords .................................................................................... 44
Features ..................................................................................... 45

**Defining the hosts** ........................................................................ 46
Key terms .................................................................................. 46
host context agent ........................................................................ 46
Hosts ...................................................................................... 46
Host groups .............................................................................. 46
Storage partitions ........................................................................ 46
Defining the hosts ........................................................................ 49

**Configuring the storage** ............................................................... 51
Key terms .................................................................................. 51
Default Group .......................................................................... 51
disk pool ............................................................................... 51
free capacity ........................................................................... 51
full disk encryption (FDE) .......................................................... 51
hot spare drive ........................................................................ 51
Redundant Array of Independent Disks (RAID) ................................ 51
storage partition ...................................................................... 52
unconfigured capacity .............................................................. 52
volume .................................................................................. 52
volume group ......................................................................... 52
Data assurance .......................................................................... 52
Capacity allocation .................................................................... 52
Disk pools and disk pool volumes ............................................... 53
Disk pool benefits .................................................................... 54
Volume groups and volumes ....................................................... 54
Host-to-volume mappings and storage partitions ............................. 55
Hot spare drives ........................................................................ 55
Drive Security .......................................................................... 55
Configuring the storage ................................................................. 56

**Installing the storage array as a boot device** .................................. 59
Boot device support .................................................................... 59
Installing the boot device ............................................................. 59
General preparation .................................................................... 59
Preparing the storage array as a boot device ................................ 60
Preparing the host ...................................................................... 61
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolving problems</td>
<td>63</td>
</tr>
<tr>
<td>Resolving problems</td>
<td>63</td>
</tr>
<tr>
<td>Correcting a partially managed storage array</td>
<td>63</td>
</tr>
<tr>
<td>Key terms</td>
<td>63</td>
</tr>
<tr>
<td>Partially managed storage arrays</td>
<td>63</td>
</tr>
<tr>
<td>Automatically adding a partially managed storage array</td>
<td>64</td>
</tr>
<tr>
<td>Copyright information</td>
<td>65</td>
</tr>
<tr>
<td>Trademark information</td>
<td>66</td>
</tr>
<tr>
<td>How to send comments about documentation and receive update notifications</td>
<td>67</td>
</tr>
</tbody>
</table>
# Deciding whether to use this guide

This guide describes key concepts related to software installation and initial configuration. This guide also provides instructions for installing the SANtricity Storage Manager® software on the Server Core platform, using silent mode, and setting up the storage array as a boot device.

Use the table below to determine whether you should use this guide or an alternative guide. These documents are available on the NetApp Support site: [NetApp Support](#).

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>See...</th>
</tr>
</thead>
</table>
| Understand key concepts related to software installation and configuration and storage provisioning | • This guide  
• SANtricity Storage Manager online help  
• SANtricity Storage Manager Concepts Guide |
| Install and provision in a Linux environment | • SANtricity Storage Manager FC Configuration and Provisioning for Linux Express Guide  
• SANtricity Storage Manager iSCSI Configuration and Provisioning for Linux Express Guide  
• SANtricity Storage Manager SAS Configuration and Provisioning for Linux Express Guide  
• SANtricity Storage Manager Infiniband Configuration and Provisioning for Linux Express Guide |
| Install and provision in a VMware environment | • SANtricity Storage Manager FC Configuration and Provisioning for VMware Express Guide  
• SANtricity Storage Manager iSCSI Configuration and Provisioning for VMware Express Guide  
• SANtricity Storage Manager SAS Configuration and Provisioning for VMware Express Guide |
| Install and provision in a Windows environment (not Windows server core) | • SANtricity Storage Manager FC Configuration and Provisioning for Windows Express Guide  
• SANtricity Storage Manager iSCSI Configuration and Provisioning for Windows Express Guide  
• SANtricity Storage Manager SAS Configuration and Provisioning for Windows Express Guide |
<p>| Install SANtricity in a Windows Server Core environment | This guide |
| Set up the storage array on a boot device | This guide |</p>
<table>
<thead>
<tr>
<th>If you want to….</th>
<th>See….</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install the Storage Manager packages using silent mode</td>
<td>This guide</td>
</tr>
<tr>
<td>Configure multipath drivers</td>
<td><em>SAN</em>tricity <em>Storage Manager Multipath Drivers Guide</em></td>
</tr>
</tbody>
</table>
Deciding on the management method

Before you install and use SANtricity Storage Manager software, you need to know which storage management method you plan to use.

Key terms

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

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.

Management methods

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

You can configure the management ports in various ways depending on:

• The management method
• The presence of a DHCP server
• The use of IPv6 stateless address auto-configuration

See Preparing to add the storage array to the management domain on page 26 for details.

Use the Key terms and the following illustrations to determine the management method you will use.

Note: The following example shows the Client running on a second host. However, the Client can run on the same host as the Agent.
Deciding on the management method

The following displays an example of in-band management topology:
The following displays an example of out-of-band management topology:
Out-of-band and in-band requirements

To determine whether to use out-of-band or in-band management, consider your requirements, advantages, and disadvantages of each method.

<table>
<thead>
<tr>
<th>Management Method</th>
<th>Requirements</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>All out-of-band methods</td>
<td>Connect separate Ethernet cables to each controller. Refer to the following three types of out-of-band methods.</td>
<td>This method does not use a logical unit number (LUN) on the host. This method does not use I/O path bandwidth for storage array management functions. You do not need to install host-agent software. This method does not use the SAS, Fibre Channel or iSCSI bandwidth for storage array management functions.</td>
<td>Ethernet cables are required. An Ethernet cable is required for additional manual network configuration. A router is required.</td>
</tr>
<tr>
<td>Out-of-band without a DHCP server</td>
<td>Manually configure the network settings on the controllers.</td>
<td>You must manually configure the network settings on the controllers. Ethernet cables are required.</td>
<td>Ethernet cables are required. An Ethernet cable is required for additional manual network configuration. A router is required.</td>
</tr>
<tr>
<td>Out-of-band – IPv6 stateless address auto-configuration without a DHCP server (IPv6 networks only)</td>
<td>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.</td>
<td>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.</td>
<td>Ethernet cables are required. An Ethernet cable is required for additional manual network configuration. A router is required.</td>
</tr>
<tr>
<td>Management Method</td>
<td>Requirements</td>
<td>Advantages</td>
<td>Disadvantages</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>Out-of-band <em>with</em> a DHCP server (IPv4 networks only)</td>
<td>Connect separate Ethernet cables to each controller.</td>
<td>No additional manual network configuration is required on the controllers.</td>
<td>Ethernet cables are required.</td>
</tr>
<tr>
<td></td>
<td>Assign either static IP addresses or dynamic IP addresses to the controllers using your DHCP server. Alternatively, the SANtricity Storage Manager Array Management Window (AMW) can be used to set the IP addresses after the storage array has been discovered. It is recommended that you either reserve the controller IPs in the DHCP server or assign a static IP address so that the management port addresses will not change if the power to the storage array is disrupted. 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: <em>xx.xx.xx.xx.xx.xx</em>.</td>
<td>By default, the controllers automatically obtain their IP addresses from the DHCP server after you turn on the power to the controller-drive tray. This method does not use a special Access Volume to communicate with the host.</td>
<td></td>
</tr>
</tbody>
</table>

- 00 A0 B8 00 00 00
- 00 A0 B8 00 00 00
- 11 12 34 56 78
- 11 12 34 56 78
<table>
<thead>
<tr>
<th>Management Method</th>
<th>Requirements</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| 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. If a firewall is installed on the I/O-attached host, ensure that port 2463 is open. | 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.  
• Is not supported on InfiniBand systems.  
• Is not supported on some OSes (VMware, OS X). |
Deciding which packages to install

Different storage management software components and packages are required for different machines.

Key terms

**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.

Host operating systems

Considerations for SANtricity Storage Manager's support of host operating systems (OSes) include OS versions, host bus adapters (HBAs), host processors, multipath drivers, JRE levels, and SANboot.

For information about compatibility of these components with SANtricity Storage Manager, see the NetApp Interoperability Matrix Tool.
Storage management software components

Depending on your configuration and data storage requirements, you select different storage management software components.

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 Out-of-band and in-band requirements on page 11). This package is required for in-band management.

Multipath driver
This package contains the multipath 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.

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 (ASUP) 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.

You must install the utilities and the multipath driver on each host attached to the storage array.

Note: Depending on your operating system, a multipath driver package may not be included with the SANtricity installer. In this case you should install a separate multipath driver. Check the IMT for a multipath driver that is supported for your configuration.
Refer to the following software configurations diagram and accompanying tables to determine which software packages to install on each machine:

![Software Configuration Diagram](image)

<table>
<thead>
<tr>
<th>Machine</th>
<th>Minimum Software Required</th>
<th>Installation Package (Choose One) (See the tables that follow)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management station</td>
<td>Client</td>
<td>• Typical Installation</td>
<td>• Click <strong>No</strong> to the prompt, <strong>Automatically start Monitor?</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Management Station</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Custom</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> Linux OS automatically starts the Event Monitor when you install the storage management software and it will continue to run until you stop it.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Machine</td>
<td>Minimum Software Required</td>
<td>Installation Package (Choose One) (See the tables that follow)</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Management station with the Storage Manager Event Monitor always running</td>
<td>Client</td>
<td>• Typical Installation</td>
<td>• Click Yes to the prompt, Automatically start Monitor?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Management Station</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Custom</td>
<td></td>
</tr>
<tr>
<td>Host (I/O only)</td>
<td>• Utilities</td>
<td>• Typical Installation</td>
<td>• All AIX I/O attach hosts require the ODM utility. This is automatically installed with the SMinstaller, or it can be downloaded as a standalone package from <a href="https://www.netapp.com/support">NetApp Support</a>.</td>
</tr>
<tr>
<td></td>
<td>• Agent</td>
<td>• Host</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multipath driver*</td>
<td>• Custom</td>
<td></td>
</tr>
<tr>
<td>Host – Also acting as an agent for the in-band management method</td>
<td>• Client (either on this host or on a machine with network access to this host)</td>
<td>• Typical Installation</td>
<td>Click No to the prompt, Automatically start Monitor?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Host (no client install)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Custom</td>
<td></td>
</tr>
<tr>
<td>Host – Also acting as a monitor for sending critical alerts</td>
<td>• Client</td>
<td>• Typical Installation</td>
<td>• Click Yes to the prompt, Automatically start Monitor?</td>
</tr>
<tr>
<td></td>
<td>• Utilities -</td>
<td>• Management Station</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Agent</td>
<td>• Custom</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multipath driver*</td>
<td>• Custom</td>
<td></td>
</tr>
<tr>
<td>Host – Also acting as an agent for the in-band management method and a monitor for sending critical alerts</td>
<td>• Client</td>
<td>• Typical Installation</td>
<td>• Click Yes to the prompt, Automatically start Monitor?</td>
</tr>
<tr>
<td></td>
<td>• Utilities</td>
<td>• Management Station</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Agent</td>
<td>• Custom</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multipath driver*</td>
<td>• Custom</td>
<td></td>
</tr>
</tbody>
</table>
*A multipath package may not be included in the SANtricity installer, depending on your OS.

<table>
<thead>
<tr>
<th>Installation wizard selections</th>
<th>Client</th>
<th>Utilities</th>
<th>Agent</th>
<th>Multipath</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical Installation</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Management Station</td>
<td>✔</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Host</td>
<td>—</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Custom (you select the components)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
SANtricity Storage Manager installation options

To use options beyond those provided in the OS- and protocol-specific Software Configuration and Provisioning Express Guides, you can follow the instructions in this topic.

The separate native installation packages are supplied with SANtricity Storage Manager in the native directory. Refer to the NetApp Interoperability Matrix Tool for updates.

Some operating systems support using the storage array as a boot device. For compatibility information, see the NetApp Interoperability Matrix at NetApp Interoperability Matrix Tool. For specific SAN boot instructions, consult your HBA vendor. Then see Installing the storage array as a boot device on page 59.

If you are running a Windows Server Core version, perform the procedures in Windows Server Core: Installing SANtricity Storage Manager on page 24.

Minimum system requirements for SANtricity Storage Manager

You must ensure the system that will contain the SANtricity Storage Manager client has the following minimum requirements:

- **RAM**: 2 GB for Java Runtime Engine
- **CPU**: Use the NetApp Interoperability Matrix Tool to confirm that your host’s architecture is supported.
- **Disk space**: 5 GB

Installing SANtricity 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 following command for your operating system:

- **Linux/Unix**: SMIA.xx.xx.xx.xx.bin -f installer.properties
- **Windows**: SMIA.xx.xx.xx.xx.exe -f installer.properties

Options for silent installation

The installer provides four options for Silent mode installation:

- All (client, agent, utils, multipath 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: \texttt{CHOSEN_INSTALL_SET=Custom1}

• To install the host configuration set: \texttt{CHOSEN_INSTALL_SET=Custom2}

• To install a customized configuration set: \texttt{CHOSEN_INSTALL_SET=Custom}

**Custom installation parameters**

These four features are available for you to install:

- SMclient
- SMagent
- SMutil
- Multipath Driver

\textit{Note:} A multipath driver package may not be included with the SANtricity installer, depending on your OS.

You can install one or more of the four features by entering the corresponding value. For example, to install only the SMclient and the SMutil, enter the parameter \texttt{CHOSEN_INSTALL_FEATURE_LIST=SMclient,SMutil}.

**The default installer.properties file**

Consider the following information about the default \texttt{installer.properties} file:

- If this file is named \texttt{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 \texttt{-f} option in the installer:

  \texttt{INSTALLER_UI=silent}

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

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

After you have determined which install set to use, enter the corresponding value. For example, to install only the SMclient enter the value:

\texttt{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, and multipath driver. For example, if you want to install only the SMclient, you would enter the following value:

\texttt{CHOSEN_INSTALL_FEATURE_LIST=SMclient}

You can specify whether or not to start the monitor service by entering either \texttt{0} for \textbf{Yes}, or \texttt{1} for \textbf{No}. For example, to start the monitor service, enter the following:

\texttt{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 command:

```bash
USER_REQUESTED_RESTART=NO
```

**Note:** If the multipath driver was removed during the uninstall, you need to set the value to **NO** and manually reboot the system.

**Note:** The auto-reboot does not work for the uninstall.

If a multipath driver is included in the install set, you can choose which multipath 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 enter the following command:

```bash
REQUESTED_FO_DRIVER=mpio
```

## AIX and VIOS: Installing E-Series entries in the ODM

The Object Data Manager (ODM) manages a database of information about the system and device configuration integrated into the AIX operating system (OS) and Virtual I/O Server (VIOS). VIOS enables you to share physical resources between logical AIX partitions. NetApp SANtricity data is stored in the ODM by the AIX. Data managed by the ODM is stored and maintained as objects with associated attributes.

**Note:** You must install the ODM package on all AIX I/O attached hosts.

**Note:** If you have installed the SMinstaller on AIX, you do not need to perform this procedure.

### Uninstalling previous E-Series entries

#### Step

1. To uninstall the previous E-Series entries package, run the following command:

```bash
> installp -ug disk.fcp.netapp_eseries.rte
```

When the previous E-Series entries package has been successfully uninstalled, a confirmation message appears:

<table>
<thead>
<tr>
<th>Installation Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>disk.fcp.netapp_eseries.rte</td>
</tr>
</tbody>
</table>

**Note:** In addition to running the uninstall command for previous E-Series entries, you must also manually remove all NetApp committed/branded hdisk from the system before running the install command for new E-Series entries.
Installing new E-Series entries

Steps

1. Download or copy the installation file, SMIA-AIX-11.25.nnnn.nnnn.bin, to a directory on your host.
   - To download the installation file, navigate to NetApp Support and download the E-Series/EF-Series SANtricity Storage Manager 11.25.nnnn.nnnn and Related Software package for AIX.

2. Change your current directory to the installation directory by typing `cd <install>` on the command line and pressing Enter.
   - `<install>` is the name of the directory on your server to which you downloaded the installation file.

3. Change the file permissions for the installer by running the `chmod 777 SMIA-AIX-11.25.*.bin` command.

4. Execute the installer by running the `.SMIA-AIX-11.25.*.bin` command.

   The following messages appear in the console window:

   ```
   Preparing to install...
   Extracting the JRE from the installer archive...
   Unpacking the JRE...
   Extracting the installation resources from the installer archive...
   Configuring the installer for this system's environment...
   Launching installer...
   Graphical installers are not supported by the VM. The console mode will be used instead...
   ==============================================================
   SANtricity (created with InstallAnywhere)
   ==============================================================
   Preparing CONSOLE Mode Installation...
   ==============================================================
   Introduction
   ----------
   The installation program will allow you to select and install the storage array host software and tools required to configure, manage, and monitor a storage array.
   Respond to each prompt to proceed to the next step in the installation.
   If you want to change something on a previous step, type 'back'.
   You may cancel this installation at any time by typing 'quit'.
   PRESS <ENTER> TO CONTINUE:
   ```

5. Press Enter when prompted.

6. Continue pressing Enter as you read through the license agreement.

7. When asked **DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N) :** enter Y to accept.

8. Based on the type of installation you are performing, select one of these options by entering the corresponding number.

   The steps in this procedure describe a typical (full) installation.

   - 1—Typical (Full Installation) (default). All of the packages are installed on the system. Choose this option if you do not know which installation type to select.
• 2—Management Station. This option is for your workstation or management computer and includes the software needed to configure, manage, and monitor a storage array.

• 3—Host. This option is for the host (server) connected to the storage array and includes the storage array server software.

• 4—Customize. This option lets you customize the features to be installed.

A pre-installation summary appears.

```
Pre-Installation Summary
------------------------
Please Review the Following Before Continuing:
Install Folder:
/opt/StorageManager
Required Disk Space
875 MB
Available Disk Space
5,032 MB
PRESS <ENTER> TO CONTINUE:
```

9. Press Enter to continue.

The installation may take several minutes. After it has completed, the following message appears:

```
Installation Complete
---------------------
Congratulations. SANtricity has been successfully installed to:
/opt/StorageManager
PRESS <ENTER> TO EXIT THE INSTALLER:
```

10. Press Enter to exit the installer.

Several files and program packages are installed to the /opt/SMgr directory and the /opt/StorageManager directory.

11. Issue a re-scan on the server by typing cfgmgr.

A re-scan allows the server to recognize the changes you have made without rebooting.

AIX uses the native MPIO (non-ALUA) for failover. After you have installed the host package, see the SANtricity Storage Manager Multipath Drivers Guide to configure the multipath driver.

Validating the ODM in AIX and VIOS

The Object Data Manager (ODM) manages a database of information about the system and device configuration integrated into the AIX and VIOS operating systems. After you install the E-Series entries package, you must validate that the ODM was updated to enable failover.

Step

1. To validate that the ODM was updated, run the following command:

```
> lslpp -l disk.fcp.netapp_eseries.rte
```

Verify the state is COMMITTED, as in the following:

```
root@ictm-iop-r12-dipper# lslpp -l disk.fcp.netapp_eseries.rte
Fileset                     Level   State     Description
----------------------------------------------------------------------
SANtricity Storage Manager installation options | 23
```
Windows Server Core: Installing SANtricity Storage Manager

Before installing SANtricity Storage Manager, you must first obtain an installation file that is specific to your operating system and to release level of the storage management software.

About this task

In the following steps, the installation file is identified as SMIA-WINx64-11.20.nnnn.nnnn.exe. The characters nnnn.nnnn are, in practice, alpha-numeric characters: for example, SMIA-WINx64-11.20.0300.0020.exe. Download this file from NetApp Support.

Steps

1. Download or copy the installation file, SMIA-WINx64-11.20.nnnn.nnnn.exe, to a directory on your host.

2. You have three options for doing the installation:

   • You can specify the `console` parameter during the installation, for example:

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

     Using this option, 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 if you need to change the installation options.

   • You can specify the `silent` parameter during the installation, for example:

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

     Using this option, 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 technical support if you need to change the installation options.

   • You can use the **SANtricity InstallAnywhere** installation. For example:

     ```
     <hsw executable>.exe
     ```

3. Change your current directory to the installation directory by typing `cd <install directory>` on the command line and then select **Enter**.

4. Type `SMIA-WINx64-11.20.nnnn.nnnn.exe`.

   The SANtricity Storage Manager InstallAnywhere dialog is displayed.

5. Press the **Next** button on the first screen of the **SANtricity Storage Manager InstallAnywhere** wizard.
The license agreement is displayed on the second screen of the wizard.

6. Select the **I accept the terms of the license agreement** radio button, then select **Next**.

The Select Installation Type screen is displayed.

7. On the **Select Installation Type** screen, select the **Typical (Full Installation)** radio button. This choice installs both the SMclient software as well as the MPIO multipath driver. Select **Next**.

The Automatically Start Monitor? screen is displayed.

8. On the **Automatically Start Monitor?** screen, select either the **Automatically start monitor** or the **Do not automatically start the monitor** radio button, then select **Next**.

The Pre-Installation Summary screen is displayed. Make note of the Install directory where the software will reside.

9. On the **Pre-Installation Summary** screen, select the **Yes, restart my system** radio button. Then select **Done**.

10. After the system reboots, make sure that the appropriate files are listed in the installation directory (for example: C:\ProgramFiles (x86)\StorageManager).

A full installation should include these directories:

- **util** (SMutil)
- **client** (SMclient)
- **agent** (SMagent)

11. Change to the **client** directory and type **SMclient.bat**.

12. For failover and other host-side setup information, see the **SANtricity Storage Manager Multipath Drivers Guide** and the SANtricity Windows express guide appropriate for your protocol.

### Solaris: Configuring the host bus adapters

A host bus adapter (HBA) resides on the host computer and provides connectivity between the host computer and the storage. HBAs free up critical server processing time. 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 Storage Manager, 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 system and multipath driver settings may be necessary to make sure that your storage array runs properly. For details, refer to **Defining the hosts** on page 46.

Refer to NetApp Interoperability Matrix at NetApp Interoperability Matrix Tool for host operating system, driver, and component compatibility information, as well as any specific configuration requirements or restrictions.

When configuring the failover or multipath driver, refer to the **SANtricity Storage Manager Multipath 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. ALUA is a feature of the controllers that provides access to a volume through any controller port.
Preparing to add the storage array to the management domain

You must prepare the storage array before adding it to the management domain.

Completing preliminary tasks for preparing the storage array

You complete some preliminary tasks before you can add the storage array to the management domain.

Make sure you have taken these steps:

• Connected all of the applicable cables.
• Turned on the power to the storage array (powering on the attached drive trays first, and then the controller-drive tray or controller tray).
• Installed the applicable storage management software.

Setting IP addresses

By default, E-Series controllers ship with DHCP enabled on both network ports. You can use the default IP addresses or assign static IP addresses.

When the network port is in a "link down" state, that is, disconnected from a LAN, the SANtricity Storage Manager reports its configuration as either static, displaying an IP address of 0.0.0.0 (earlier releases), or DHCP enabled with no IP address reported (later releases). After the network port is in a "link up" state (that is, connected to a LAN), it attempts to obtain an IP address through DHCP.

If the controller is unable to obtain a DHCP address on a given network port, it reverts to a default IP address, which may take up to 3 minutes. The default IP addresses are as follows:

| Controller 1 (port 1): IP Address: 192.168.128.101 |
| Controller 1 (port 2): IP Address: 192.168.129.101 |
| Controller 2 (port 1): IP Address: 192.168.128.102 |
| Controller 2 (port 2): IP Address: 192.168.129.102 |

When assigning IP addresses:

• Reserve Port 2 on the controllers for Customer Support usage. Do not change the default network settings (DHCP enabled).
• To set static IP addresses, use SANtricity Storage Manager. After a static IP address is configured, it remains set through all link down/up events.
• To use DHCP to assign the IP address of the controller, connect the controller to a network that can process DHCP requests. Use a permanent DHCP lease.
Note: The default addresses are not persisted across link down events. When a network port on a controller is set to use DHCP, the controller attempts to obtain a DHCP address on every link up event, including cable insertions, reboots, and power cycles. Any time a DHCP attempt fails, the default static IP address for that port is used.

Naming the storage array

You have some flexibility and some specific requirements when naming your storage array.

Take note of the following when naming your storage array:

- You can use letters, numbers, and the special characters underscore (_), hyphen (-), and pound sign (#). No other special characters are permitted.
- Limit the name to 30 characters. Any leading and trailing spaces in the name are deleted.
- Use a unique, meaningful name that is easy to understand and to remember. Avoid arbitrary names or names that would quickly lose their meaning in the future. The prefix “Storage Array” is automatically added to the name you assign. The full name is shown in the Logical pane and in the Enterprise Management Window. For example, if you named the storage array “Engineering,” it appears as “Storage Array Engineering.”
- The storage management software does not check for duplicate names. Check the Enterprise Management Window to make sure that the name you have chosen is not used by another storage array.
- When you first discover a storage array or manually add it, the storage array will have a default name of “unnamed.”
**Adding the storage array to the management domain**

You can choose from several methods for adding the storage array to the management domain. The appropriate method depends on your network configuration and how you initially configured the controllers.

---

**Choosing the method for adding the storage array to the management domain**

You decided what kind of method to use in *Deciding on the management method* on page 8. See the following table to determine the correct procedure to use to add the storage array to the management domain.

<table>
<thead>
<tr>
<th>If you are...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Using out-of-band management and DHCP addressing of the management ports, and the management station is on the same subnetwork as the array. • Using out-of-band IPv6 stateless address auto-configuration without a DHCP server (IPv6 networks only) and the management station is on the same subnetwork as the storage.</td>
<td>See <em>Using automatic discovery: Out-of-band management</em> on page 29.</td>
</tr>
<tr>
<td>• Using out-of-band management and DHCP addressing of the management ports, and you will get the controller management port IP addresses from the DHCP servers to add the array to the management domain. • Using out-of-band IPv6 stateless address auto-configuration without a DHCP server (IPv6 networks only) and the management station is NOT on the same subnetwork as the storage.</td>
<td>See <em>Manually adding a storage array: Out-of-band management</em> on page 31.</td>
</tr>
<tr>
<td>Using DHCP addressing of the management ports for initial discovery of the array, and then switching to use static management port addressing.</td>
<td>See <em>Using DHCP and then changing to static addressing</em> on page 30.</td>
</tr>
<tr>
<td>Using out-of-band management and want to configure DHCP addressing of the management ports. You previously used the appropriate <em>Express Guide</em> for your operating system and initially configured the management ports to use the default IP addresses.</td>
<td>See <em>Configuring DHCP addressing</em> on page 32.</td>
</tr>
</tbody>
</table>
If you are... | Do this...
--- | ---
Using out-of-band management and will not be using DHCP addressing. You are not using IPv6 stateless address auto-configuration. Your management station is not on the same subnetwork as the storage array. | Choose one of the following options:
- Use in-band management temporarily to configure the controllers. This option is for Fibre Channel and SAS environments only. See *Manually configuring the controllers by using the in-band method initially* on page 34.
- Temporarily set up a private network to configure the controller management ports. You will first need to configure the management station so that it resides on the same subnetwork during controller management IP configuration. See *Manually configuring the controllers by setting up a temporary private network* on page 36.

Using in-band management. | See *Adding the storage array for in-band management* on page 33.

---

**Using automatic discovery: Out-of-band management**

**Before you begin**

- The management station must be attached to the same subnet as the storage.
- Ethernet cables must be attached to each controller.
- The DHCP server must be configured to assign a permanent (static) DHCP lease.
- If you are using IPv6 stateless address auto configuration without a DHCP server, you must have connected at least one router for sending the IPv6 network address prefix in the form of router advertisements. 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.

**Steps**

1. Open the *SANtricity Storage Manager*.

   The *Enterprise Management Window (EMW)* is displayed.

   **Note:** When you open *SANtricity Storage Manager* for the first time, the Select Addition Method screen prompts you to select whether you want to choose the *Automatic* or *Manual* method to add a new storage array.

2. On the Select Addition Method screen, select the Automatic radio button, and then select OK.

   This process finds all of the storage arrays on the local sub-network. Several minutes might lapse to complete the process.

3. In the EMW Devices tab, double-click the storage array to open the *Array Management Window (AMW)*.

   When you open the AMW for the first time, the Disk Pool Automatic Configuration screen is displayed. Select No to dismiss the wizard and name the storage array.
4. Name the storage array.
   a. In the **EMW Setup** tab, select **Name/Rename Storage Arrays**.
   b. In the **Select storage array** list, select the storage array you added.
   c. In the **Storage array name** field, type a name for the storage array. Storage array names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens(-), and pound signs (#). Choose a descriptive name for the storage array to make it easier for data center administrators to manage the storage resources over time.

5. Go to *Configuring other SANtricity options* on page 41 to continue setting up the storage array.

### Using DHCP and then changing to static addressing

**Before you begin**

- The management station must be attached to the same subnet as the storage.
- An ethernet cables must be attached to each controller.

**Steps**

1. Open the **SANtricity Storage Manager**.
   The **Enterprise Management Window (EMW)** is displayed.
   **Note:** When you open SANtricity Storage Manager for the first time, the **Select Addition Method** screen prompts you to select whether you want to choose the **Automatic** or **Manual** method to add a new storage array.

2. On the **Select Addition Method** screen, select the **Automatic** radio button, and then select **OK**.
   This process finds all of the storage arrays on the local sub-network. Several minutes might lapse to complete the process.

3. In the **EMW Devices** tab, double-click the storage array to open the **Array Management Window (AMW)**.
   When you open the **AMW** for the first time, the **Disk Pool Automatic Configuration** screen is displayed. Select **No** to dismiss the wizard.

4. Name the storage array.
   a. In the **EMW Setup** tab, select **Name/Rename Storage Arrays**.
   b. In the **Select storage array** list, select the storage array you added.
   c. In the **Storage array name** field, type a name for the storage array. Storage array names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens(-), and pound signs (#). Choose a descriptive name for the storage array to make it easier for data center administrators to manage the storage resources over time.

5. Configure the network configuration information of the controllers, using information you obtain from your network administrator.
   a. Select the **Hardware** tab in the **AMW**.
   b. Select **Hardware > Controller > Configure > Management Ports**.
c. On the **Change Network Configuration** dialog box, select Controller A, Port 1 in the **Ethernet port** drop-down list.

d. 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**.

e. Depending on the format of your network configuration information, select the **Enable IPv4** check box, the **Enable IPv6** check box, or both check boxes.

f. Depending on the format 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.

g. Select Controller B, Port 1 in the **Ethernet port** drop-down list, and repeat step c through step f for controller B.

h. Select **OK**.

6. Return to the **EMW**, select the storage array, and then select **Edit > Remove > Storage Array**.

7. On the **EMW Setup** tab, select **Add Storage Arrays**.

8. On the **Select Addition Method** dialog box, select the **Manual** radio button.

9. On the **Add New Storage Array - Manual** screen, make sure that the default **Out-of-band management** radio button is selected. Enter the IP address assigned to controller A, port 1, and controller B, port 1, on the storage array you are adding.

10. Go to *Configuring other SANtricity options* on page 41 to continue setting up the storage array.

---

### Manually adding a storage array: Out-of-band management

**Before you begin**

- If you are using DHCP, the DHCP server is configured to assign a permanent (static) DHCP lease. You must have obtained the IP addresses of the controller management ports from the DHCP server.

- If you are using IPv6 stateless address auto-configuration without a DHCP server, you have connected at least one router for sending the IPv6 network address prefix in the form of router advertisements. You must have obtained the IP addresses of the controllers.

**Steps**

1. Open **SANtricity Storage Manager**.

   The **Enterprise Management Window (EMW)** is displayed.

   **Note:** When you open SANtricity Storage Manager for the first time, the **Select Addition Method** screen prompts you to select whether you want to choose the **Automatic** or **Manual** method to add a new storage array.

2. On the **Select Addition Method** screen, select the **Manual** radio button, and then select **OK**.
3. On the **Add New Storage Array - Manual** screen, make sure that the default **Out-of-band management** radio button is selected. Enter the IP address assigned to controller A, port 1, and controller B, port 1, on the storage array you are adding.

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

   **Note:** Alternatively, you can enter the DNS/network name of each controller.

4. Select **Add**.

5. On the **Storage Array Added** screen, select **No** to finish adding storage arrays.

6. In the **EMW Devices** tab, double-click the storage array to open the **Array Management Window (AMW)**.

   When you open the AMW for the first time, the **Disk Pool Automatic Configuration** screen is displayed. Select **No** to dismiss the wizard and finish setting up the management IP addresses.

7. Name the storage array.
   a. In the **EMW Setup** tab, select **Name/Rename Storage Arrays**.
   b. In the **Select storage array** list, select the storage array you added.
   c. In the **Storage array name** field, type a name for the storage array. Storage array names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens(-), and pound signs (#). Choose a descriptive name for the storage array to make it easier for data center administrators to manage the storage resources over time.
   d. Select **OK**.

8. Go to *Configuring other SANtricity options* on page 41 to continue setting up the storage array.

### Configuring DHCP addressing

You change the storage array management ports that you configured using the appropriate *Express Guide* for your operating system and host protocol from static addressing to DHCP addressing.

**Steps**

1. Disconnect the private network you set up using the appropriate *Express Guide* for your operating system, change your management station to connect to your regular network, and prepare the DHCP server.
   a. Make sure your DHCP server is connected to your regular network and that it is configured to assign a permanent (static) DHCP lease.
   b. Connect an Ethernet cable to the management station and to management port 1 on either controller (A or B). Wait 3 minutes for the controller's default DHCP setting to time out.
      
      **Note:** Reserve port 2 on the controller for maintenance operations.
   c. Change the management station to use DHCP. Refer to your operating system documentation for instructions on how to change the network settings on the management station and how to verify that the address has changed.

2. Open the **SANtricity Storage Manager**.

   The **Enterprise Management Window (EMW)** is displayed.
Note: When you open SANtricity Storage Manager for the first time, the Select Addition Method screen prompts you to select whether you want to choose the Automatic or Manual method to add a new storage array.

3. On the Select Addition Method screen, select the Automatic radio button, and then select OK.
This process finds all of the storage arrays on the local sub-network. Several minutes might lapse to complete the process.

4. In the EMW Devices tab, double-click the storage array to open the Array Management Window (AMW).
When you open the AMW for the first time, the Disk Pool Automatic Configuration screen is displayed. Select No to dismiss the wizard and name the storage array.

5. Name the storage array.
   a. In the EMW Setup tab, select Name/Rename Storage Arrays.
   b. In the Select storage array list, select the storage array you added.
   c. In the Storage array name field, type a name for the storage array. Storage array names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens(-), and pound signs (#). Choose a descriptive name for the storage array to make it easier for data center administrators to manage the storage resources over time.

6. Go to Configuring other SANtricity options on page 41 to continue setting up the storage array.

Adding the storage array for in-band management

Before you begin

- The host agent software must be installed on a host attached to the storage array.
- You must know the host name or IP address of this host.
- For Red Hat Linux 7.1 (RHEL 7.1): You must have load the sg driver to ensure that SANtricity Storage Manager can discover the management LUN. If the sg driver is not loaded, in-band management does not function.

Steps

1. Open the SANtricity Storage Manager.
   The Enterprise Management Window (EMW) is displayed.
   Note: When you open SANtricity Storage Manager for the first time, the Select Addition Method screen prompts you to select whether you want to choose the Automatic or Manual method to add a new storage array.

2. On the Select Addition Method screen, select the Manual radio button, and then select OK.

3. On the Add New Storage Array - Manual screen, select the In-band management radio button. Enter the host name or IP address of the host that is running the host-agent software, and select Add.
   Note: You can enter the IP addresses in either the IPv4 format or the IPv6 format.

4. On the Storage Array Added screen, select No to finish adding storage arrays.
5. In the **EMW Devices** tab, double-click the storage array to open the **Array Management Window (AMW)**.

When you open the **AMW** for the first time, the **Disk Pool Automatic Configuration** screen is displayed. Select **No** to dismiss the wizard and finish setting up the management IP addresses.

6. Name the storage array.
   a. In the **EMW Setup** tab, select **Name/Rename Storage Arrays**.
   b. In the **Select storage array** list, select the storage array you added.
   c. In the **Storage array name** field, type a name for the storage array. Storage array names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens(-), and pound signs (#). Choose a descriptive name for the storage array to make it easier for data center administrators to manage the storage resources over time.
   d. Select **OK**.

7. Go to *Configuring other SANtricity options* on page 41 to continue setting up the storage array.

### Manually configuring the controllers by using the in-band method initially

**Before you begin**

The prerequisites for this procedure include:

- The host agent software is installed on a host attached to the storage array.
- You know the host name or IP address of this host.
- You have obtained the network configuration information from your network administrator for the controllers (IP address, subnet mask, and gateway or IP address and routable IP address).

**Note:** This method does not work if the controller-drive tray uses an iSCSI protocol. When you initially configure an array in this environment, there are no IP addresses set up on the iSCSI ports, required for iSCSI sessions from the host to the storage array and in-band management. If you use iSCSI protocol, see *Manually configuring the controllers by setting up a temporary private network* on page 36.

**Steps**

1. Open the SANtricity Storage Manager.
   
   The **Enterprise Management Window (EMW)** is displayed.
   
   **Note:** When you open SANtricity Storage Manager for the first time, the **Select Addition Method** screen prompts you to select whether you want to choose the **Automatic** or **Manual** method to add a new storage array.

2. On the **Select Addition Method** screen, select the **Manual** radio button, and then select **OK**.

3. On the **Add New Storage Array - Manual** screen, select the **In-band management** radio button. Enter the host name or IP address of the host that is running the host-agent software, and select **Add**.
   
   **Note:** You can enter the IP addresses in either the IPv4 format or the IPv6 format.
4. On the **Storage Array Added** screen, select **No** to finish adding storage arrays.

5. In the **EMW Devices** tab, double-click the storage array to open the **Array Management Window (AMW)**.

   When you open the **AMW** for the first time, the **Disk Pool Automatic Configuration** screen is displayed. Select **No** to dismiss the wizard and finish setting up the management IP addresses.

6. Name the storage array.
   a. In the **EMW Setup** tab, select **Name/Rename Storage Arrays**.
   b. In the **Select storage array** list, select the storage array you added.
   c. In the **Storage array name** field, type a name for the storage array. Storage array names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens(-), and pound signs (#). Choose a descriptive name for the storage array to make it easier for data center administrators to manage the storage resources over time.
   d. Select **OK**.

7. Configure the network configuration information of the controllers, using information you obtain from your network administrator.
   a. Select the **Hardware** tab in the AMW.
   b. Select **Hardware > Controller > Configure > Management Ports**.
   c. On the **Change Network Configuration** dialog box, select Controller A, Port 1 in the **Ethernet port** drop-down list.
   d. 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**.
   e. Depending on the format of your network configuration information, select the **Enable IPv4** check box, the **Enable IPv6** check box, or both check boxes.
   f. Depending on the format 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.
   g. Select Controller B, Port 1 in the **Ethernet port** drop-down list, and repeat step c through step f for controller B.
   h. Select **OK**.

8. Return to the **EMW**, select the storage array, and then select **Edit > Remove > Storage Array**.

9. On the **EMW Setup** tab, select **Add Storage Arrays**.

10. On the **Select Addition Method** dialog box, select the **Manual** radio button.

11. On the **Add New Storage Array - Manual** screen, make sure that the default **Out-of-band management** radio button is selected. Enter the IP address assigned to controller A, port 1, and controller B, port 1, on the storage array you are adding.

12. Go to **Configuring other SANtricity options** on page 41 to continue setting up the storage array.
Manually configuring the controllers by setting up a temporary private network

Before you begin

The prerequisites for this procedure include:

- You have connected the management station directly into Ethernet port 1 on each controller.
- You have connected an ethernet cable to the management station and to the management port 1 on either controller (A or B).
  
  **Note:** Reserve port 2 on the controller for maintenance operations.

- You have obtained the network configuration information from your network administrator for the controllers (IP address, subnet mask, and gateway or IP address and routable IP address).

  **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.

Steps

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.

   a. 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.

      **Note:** 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.

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

   c. 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.

   d. From a command prompt, ping the controller IPs to make sure they are accessible.
Example

```bash
> ping 192.168.128.102
```

Reply from 192.168.128.102: bytes = 32 time<1ms TTL = 64

Ping statistics for 192.168.128.102:

Packets: Sent = 4, Received =4, Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0 ms

2. Open the SANtricity Storage Manager.

   The Enterprise Management Window (EMW) is displayed.

   **Note:** When you open SANtricity Storage Manager for the first time, the **Select Addition Method** screen prompts you to select whether you want to choose the **Automatic** or **Manual** method to add a new storage array.

3. On the **Select Addition Method** screen, select the **Automatic** radio button, and then select **OK**.

   This process finds all the storage arrays on the local sub-network. Several minutes might lapse to complete the process.

4. In the **EMW Devices** tab, double-click the storage array to open the **Array Management Window (AMW)**.

   When you open the AMW for the first time, the **Disk Pool Automatic Configuration** screen is displayed. Select **No** to dismiss the wizard and finish setting up the management IP addresses.

5. Name the storage array.

   a. In the **EMW Setup** tab, select **Name/Rename Storage Arrays**.

   b. In the **Select storage array** list, select the storage array you added.

   c. In the **Storage array name** field, type a name for the storage array. Storage array names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens(-), and pound signs (#). Choose a descriptive name for the storage array to make it easier for data center administrators to manage the storage resources over time.

   d. Select **OK**.

6. Configure the network configuration information of the controllers, using information you obtain from your network administrator.

   a. Select the **Hardware** tab in the AMW.

   b. Select **Hardware > Controller > Configure > Management Ports**.

   c. On the **Change Network Configuration** dialog box, select Controller A, Port 1 in the **Ethernet port** drop-down list.

   d. From the **Speed and duplex mode** drop-down list, select **Auto-negotiate**.
Note: Attention Possible Connectivity Issues – After you select Auto-negotiate, make sure that your Ethernet switch also is set to Auto-negotiate.

e. Depending on the format of your network configuration information, select the Enable IPv4 check box, the Enable IPv6 check box, or both check boxes.

f. Depending on the format 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.

g. Select Controller B, Port 1 in the Ethernet port drop-down list, and repeat step c through step f for controller B.

h. Select OK.

7. Disconnect the Ethernet cable from your management station, and reconnect the Ethernet cables from the controllers into your regular network.

8. Complete the steps necessary to change the management station’s IP address back to what it was initially.

9. Go to Configuring other SANtricity options on page 41 to continue setting up the storage array.

Using the Service Interface to set IPs

The Serial Port Recovery Interface, also known as the Service Interface, allows you to configure controllers manually.

Before you begin

• A terminal emulator program must be installed on the management station.

• You must have a serial cable.

• You must have functional knowledge of the following concepts:
  ◦ Terminal emulator usage
  ◦ Executing break sequences
  ◦ Cycling baud rates

Steps

1. Connect to the controller's serial port.

2. Send a BREAK code.

   The controller's serial port converts to active state.

3. Enter <S> at the following prompt to initiate the Service Interface:

   Press within 5 seconds: <S> for Service Interface. <BREAK> for baud rate

   Note: The above command prompts must be entered as uppercase.

   A prompt for the Service Interface password is displayed.
4. Enter **SPRIentry** at the following Service Interface password prompt:

```
Enter Password to access Service Interface (60 sec timeout): SPRIentry
```

**Note:** If a password is not entered within the 60 second interval, the process times out.

The Service Interface Main Menu displays.

5. Under the Service Interface Main Menu, enter 2 to select Change IP Configuration.

The Select Ethernet Port menu displays.

6. From the Select Ethernet Port menu, enter 1 to select Ethernet Port 1.

The Change IP Configuration menu displays.

7. Under the Change IP Configuration menu, enter the following to enable the IPv4 protocol for the port:

```
Enable IPv4? (Y/N): Y
```

8. Under Configure using DHCP?, enter the following:

```
Configure using DHCP? (Y/N): N
```

The current fixed IP address, IP subnet mask, and IP address of the default gateway associated with the controller port is displayed under the Current Configuration column within the Change IP Configuration menu.

9. To configure the fixed IP address used for the controller port, enter the appropriate data under the New Configuration column for the IP Address field.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Current Configuration</th>
<th>New Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>if0</td>
<td>10.113.160.252</td>
<td>10.113.160.226</td>
</tr>
</tbody>
</table>

**Note:** You can delete entries under the New Configuration column by pressing '.'

10. To configure the IP subnet mask associated with the controller port, enter the appropriate data under the New Configuration column for the Subnet Mask field.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Current Configuration</th>
<th>New Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>if0</td>
<td>255.255.252.0</td>
<td>255.255.242.0</td>
</tr>
</tbody>
</table>

11. To configure the IP address for the default gateway associated with the controller port, enter the appropriate data under the New Configuration column for the Gateway IP Address field.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Current Configuration</th>
<th>New Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>if0</td>
<td>10.113.160.1</td>
<td>10.113.157.1</td>
</tr>
</tbody>
</table>

12. Under Change port configuration (speed & duplex)?, enter the following:

```
Change port configuration (speed & duplex)? (Y/N): N
```
13. **Under Reboot to have the settings take effect?, enter the following:**

   Reboot to have the settings take effect? (Y/N): N  

   **Note:** Reboot will still be required for changes to take effect.

14. Press ENTER and then ^D.

   All changes made within the Change IP Configuration prompt are applied, and the Service Interface Main Menu is displayed.

15. **Under the Service Interface Main Menu, enter q to select Quit Menu.**

   The Service Interface closes.
Configuring other SANtricity options

In this section, you learn about the Enterprise Management Window and Array Management Window Setup tabs and some key concepts for alert notification, setting a storage array password, and managing premium features. You use the SANtricity Storage Manager, including the online help topics, to perform the tasks. The tasks included below provide a reference to the menu or tab in SANtricity Storage Manager.

<table>
<thead>
<tr>
<th>Initial Configuration Task</th>
<th>SANtricity menu or tab option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the delivery method for AutoSupport messages</td>
<td>From the Enterprise Management Window, select the Devices tab, select Discovered Storage Arrays, and then select Tools &gt; AutoSupport &gt; Configuration. Use the SANtricity online help if needed to complete the task.</td>
</tr>
<tr>
<td>Setting alert notifications</td>
<td>From the Enterprise Management Window, select the Devices tab, select a node and then select Edit &gt; Configure Alerts. Use the SANtricity online help if needed to complete the task.</td>
</tr>
<tr>
<td>Setting up a storage array password</td>
<td>From the Array Management Window, select Storage Array &gt; Security &gt; Set Password. Use the SANtricity online help if needed to complete the task.</td>
</tr>
<tr>
<td>Managing premium features</td>
<td>From the Array Management Window, select Storage Array &gt; Premium Features. Use the SANtricity online help if needed to complete the task.</td>
</tr>
</tbody>
</table>

Enterprise Management Window and Array Management Window

SANtricity Storage Manager has two main windows that allow you to view your storage system and individual arrays within the system.

<table>
<thead>
<tr>
<th>User Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Management Window</td>
<td>Appears when you first start SANtricity Storage Manager. Provides a view of all of the storage arrays, including the partially managed storage arrays, in your management domain. Allows you to automatically or manually add and remove storage arrays, set alert notifications (through either AutoSupport [ASUP] messages or email and SNMP), and perform other high-level configuration functions. 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. Allows you to manage and configure an individual storage array by launching the Array Management Window.</td>
</tr>
<tr>
<td>User Interface</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Array Management Window</td>
<td>Launches from the Enterprise Management Window to manage an individual storage array. Provides all the functions to configure, maintain, and troubleshoot an individual storage array. Multiple Array Management Windows can appear at the same time (one for each storage array you want to manage).</td>
</tr>
<tr>
<td>Enterprise Management Window Setup Tab and Array Management Window Setup Tab</td>
<td>When you first start the Enterprise Management Window, its <strong>Setup</strong> tab is selected by default. When you first start the Array Management Window, its <strong>Setup</strong> tab is selected by default. The <strong>Setup</strong> tabs provide quick access to common setup tasks. The tasks shown are different, depending on the window from which the <strong>Setup</strong> tab was launched.</td>
</tr>
</tbody>
</table>

The following displays an example of the Enterprise Management Window (EMW) with the Setup tab selected:
The following displays an example of the Array Management Window (AMW) with the Setup tab selected:

**Note:** "Configure iSCSI Host Ports" and "Manage iSCSI Settings" appear only if your configuration is using iSCSI network protocols.

### 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 ASUP data is compressed into a single compressed archive file format (7z) at the location you specify.

You can choose between two methods of collecting support data: 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**
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.

**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 storage 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.

**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.

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.

Follow these guidelines for setting passwords:

• For increased protection, use a long password with at least 15 alphanumeric characters. The maximum password length is 30 characters.

• Passwords are case sensitive.

• 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.

### Features

You enable a feature through a feature key file that you obtain from NetApp Support Site at [NetApp Support](https://www.netapp.com/support). The feature is either enabled or disabled.
Defining the hosts

**Note:** If you will not use storage partitions, you can skip the information about *Host groups* on page 46 and *Storage partitions* on page 46, and go to *Defining the hosts* on page 49.

**Note:** You must know the unique initiator port name of each HBA port (World Wide Port Names in the case of FC). See the HBA utility or operating system documentation for instructions to obtain these unique initiator or WWPN port names.

### Key terms

**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.

### 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.

**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.

### 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 *Defining the hosts* on page 49.

### 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.

- 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:
  ◦ 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:** When you have multiple hosts accessing the volumes in a storage partition, you must have some type of clustering software on the hosts to manage volume sharing and accessibility.

The following displays an example of no additional storage partitions required:

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

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

• You do need to create storage partitions if these conditions exist:
  ◦ You want certain hosts to access only certain volumes.
The following displays an 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.

- 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.
Defining the hosts

Steps

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. If you are setting up an iSCSI environment, from the Setup tab on the Array Management Window, select **Configure iSCSI Host Ports**.

   If the storage array does not contain a 10Gb host interface card, change the default value of the **Configure Ethernet port speed** drop-down list from 10 Gbps to 1 Gbps.

4. From the Setup tab on the Array Management Window, click **Manually Define Hosts**.

5. 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 multipathing.
Configuring the storage

You can group and manage your storage within the storage array for maximum efficiency.

Key terms

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

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 a volume 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
A spare drive that contains no data and that acts as a standby in case a drive fails in a Redundant Array of Independent Disks (RAID) Level 1, RAID Level 3, RAID Level 5, or RAID Level 6 volume. The hot spare drive can replace the failed drive in the volume. Hot spare drives are used only in volume groups, not disk pools.

Redundant Array of Independent Disks (RAID)
CONTEXT [Storage System] A disk array in which part of the physical storage capacity is used to store redundant information about user data stored on the remainder of the storage capacity. The redundant information enables 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.

**Data assurance**

The Data Assurance (DA) feature increases data integrity across the entire storage system. DA enables the storage array to check for errors that might occur when data is moved between the hosts and the drives. When this feature is enabled, the storage array appends error-checking codes (also known as cyclic redundancy checks or CRCs) to each block of data in the volume. After a data block is moved, the storage array uses these CRC codes to determine if any errors occurred during transmission. Potentially corrupted data is neither written to disk nor returned to the host.

If you want to use the DA feature, start with a volume group or disk pool that includes only drives that support DA. Then, create DA-capable volumes. Finally, map these DA-capable volumes to the host using an I/O interface that is capable of DA. I/O interfaces that are capable of DA include Fibre Channel, SAS, and iSER InfiniBand (iSCSI Extensions for RDMA/IB). DA is not supported by iSCSI over TCP/IP, or by the SRP InfiniBand.

If you choose to create a DA-enabled volume group, select the **Enable Data Assurance (DA) protection on the new volume** check box. This check box appears only if the drives, the controller, and the host bus adapter all support DA.

**Note:** If a volume group or disk pool is DA-capable and contains a DA-enabled volume, use only DA-capable drives for hot spare coverage. A volume group or disk pool that is not DA-capable cannot contain a DA-enabled volume.

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

**Capacity allocation**

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.

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.

### 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.

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

- **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.

### 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.

  **Note:** If you choose to copy a Data Assurance (DA)-enabled source volume to a target volume that is not DA enabled, you are prompted to confirm your choice. The copy can be completed, but the resulting copy is not DA enabled. For more information about how volume copy is affected by DA-enabled volumes, refer to the online help for SANtricity Storage Manager.

- 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.

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.

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.

**Note:** Hot spare drives are supported in volume groups, but they are not supported in disk pools.

Drive Security

Drive Security is a feature that prevents unauthorized access to the data on a drive that is physically removed from the storage array. A security-capable drive encrypts data during writes and decrypts data during reads using a unique encryption key. Security-capable drives can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.

To implement Drive Security, perform these steps:

1. Equip your storage array with security-capable drives: either FDE drives or FIPS drives.
2. Enable the Drive Security premium feature via a premium feature key obtained from your storage vendor.

3. Create a security key that is used by the controller to provide read/write access to the drives.

4. Create a security-enabled disk pool or volume group.

   **Attention:** Possible loss of data access – When a disk pool or volume group is secured, the only way to remove security is to delete the disk pool or volume group. Deleting the disk pool or volume group deletes all of the data in the volumes that it contains.

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. When you create a secure disk pool or volume group from security-capable drives, the drives in that disk pool or volume group become security enabled. When a security-capable 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. Furthermore, if you have both FDE drives and FIPS drives, they also 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 security-capable drive works like any other drive until it is security enabled.

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

You can erase security-enabled drives so that you can reuse the drives in another disk pool, volume group, or in another storage array. When you erase security-enabled drives, you make sure that the data cannot be read. When all of the drives that you have selected in the Physical pane are security enabled, and none of the selected drives is part of a disk pool or volume group, the Secure Erase option appears in the Drive menu.

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

### Configuring the storage

**Steps**

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**, select **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, Configure hot spares (volume groups only), Create volume groups, or Create SSD Cache (only available when SSD drives are present).

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.

Configure hot spares (volume groups only) – 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.

Create volume groups – This method creates volume groups, a set of drives to provide capacity, and a RAID level for one or more volumes. 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.

Create SSD Cache - This method creates SSD Cache, a set of Solid-State Disk (SSD) drives that you logically group together in your storage array to improve read-only performance. This option is only available if you have SSD drives in your system.

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 **Host Mappings** tab.

   b. Specify the applicable host or host group, volumes, and LUNs.

   c. Select **Host Mappings > Define**, and click **Storage Partition**.

   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.

**Note:** After you configure the volume, you can change the cache memory settings of the volume. See the online help for SANtricity Storage Manager.
Installing the storage array as a boot device

You can set up the storage array as a 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>
<thead>
<tr>
<th>Operating System</th>
<th>Boot Device Support</th>
<th>Recommended number of paths for installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Yes, where supported by the HBAs</td>
<td>1 (works with 2, but 1 is recommended)</td>
</tr>
<tr>
<td>Solaris</td>
<td>Yes, where supported by the HBAs</td>
<td>2</td>
</tr>
<tr>
<td>HP-UX</td>
<td>Yes, where supported by the HBAs</td>
<td>2</td>
</tr>
<tr>
<td>Linux</td>
<td>Yes, where supported by the HBAs</td>
<td>2</td>
</tr>
<tr>
<td>VMware</td>
<td>Yes, where supported by the HBAs</td>
<td>2</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>No</td>
<td>1</td>
</tr>
<tr>
<td>AIX</td>
<td>Yes, where supported by the HBAs</td>
<td>2</td>
</tr>
</tbody>
</table>

Installing the boot device

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

NetApp recommends using LUN 0 for booting and some operating systems may require it.

General preparation

About this task

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

Steps

1. Perform the instructions in Preparing the storage array as a boot device.
2. Perform the instructions in Preparing the host on page 61.

Result

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 technical support.

Preparing the storage array as a boot device

About this task

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

Starting the SMclient software

Steps

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 window and the Select Addition Method dialog box appear:

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

3. Select Edit > Add Storage Array.

   The Add New Storage Array dialog box 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.

Configuring the boot volume on the storage array

Steps

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 on the storage array.

   Note: You cannot create a volume on an Unconfigured Capacity node. You must create a volume on a Free Capacity node.
Note: If you do not have at least 2 GB of capacity on a Free Capacity node, you need to free enough capacity for the boot volume before you can continue. Refer to the SANtricity Storage Manager Concepts Guide or the SANtricity online help for information about freeing capacity.

5. Go to Preparing to add the storage array to the management domain.

Configuring the boot volume on a free capacity node

Steps

1. Right-click the Free Capacity node that you want to use, and click Create Volume.

   The Create Volume Specify Parameters dialog appears.

2. On the Create Volume Specify Parameters dialog, select the choices that are appropriate for the boot volume.

   a. If you are creating the volume on a disk pool, leave the Create thin volume checkbox unchecked.

      Note: If you are creating the volume from a volume group, the Create thin volume checkbox will not appear.

   b. Select the appropriate unit for the new volume capacity from the drop-down list, and the new volume capacity.

      Note: A capacity of 4 GB is recommended. Consult your operating system documentation for information on the amount of space needed for the operating system. A minimum of 2 GB is required.

   c. Enter the volume name.

      Note: The volume name must not exceed 30 characters and cannot contain spaces. Use underscores or dashes to separate elements within the volume name (for example, Boot_Volume).

   d. In the Map to host drop-down, select the Map Later option.

   e. Specify the Quality of Service attributes. Use the onscreen flyovers and the SANtricity online help system to get more information about particular attributes.

      Note: If you are creating the volume from a volume group, select the File System choice for the Volume I/O characteristic.

3. Select Finish to create the volume.

4. Use the Storage Partition feature to map the volume to the host by using LUN 0.

   Note: For additional information about how to map volumes that use Storage Partitions, refer to the online help topics in the Array Management Window.

5. If your host supports asynchronous logical unit access (ALUA), go to Preparing the host on page 61.

Preparing the host

About this task

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.

**Steps**

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.
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.

Steps

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.
   • Needs Attention – Go to step 5.
   • Unresponsive – Refer to the online help topics in the Enterprise Management Window for the procedure.
5. From the AMW, select Monitor > Health > View Health (Recovery Guru) to launch the Recovery Guru. Follow the steps in the Recovery Guru to resolve the problem.

Correcting a partially managed storage array

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

Key terms

partially managed storage array

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

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.

**Automatically adding a partially managed storage array**

**About this task**

These steps are for out-of-band partially managed storage arrays only. For in-band partially managed storage arrays, verify the connection, and refer to the SANtricity Storage Manager online help topic “Rescanning a Host for a New Storage Array” for more information on rescanning the host.

**Steps**

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.
Copyright information

Copyright © 1994–2016 NetApp, Inc. All rights reserved. Printed in the U.S.

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.

The product described in this manual may be protected by one or more U.S. patents, foreign patents,
or pending applications.

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, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx.
How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

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.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

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