



SANtricity® 11.40

Installing and Configuring for VMware®

Power Guide for Advanced Users

September 2017 | 215-11890_A0
doccomments@netapp.com

 **NetApp®**

Contents

Deciding whether to use this Power Guide	5
Configuration options	6
Configuration worksheet	10
Deciding on the management method	12
Management methods	12
Out-of-band and in-band requirements	12
Installing SANtricity Storage Manager	16
Installing the storage array as a boot device	16
Installing SANtricity Storage Manager packages using silent mode	17
Deciding which packages to install	17
Host operating systems	17
Storage management software components	17
Installing the SANtricity software on hosts, monitors, and management stations	19
Adding the storage array to the management domain	21
Preparing to add the storage array to the management domain	21
Completing preliminary tasks for preparing the storage array	21
Setting IP addresses	21
Naming the storage array	22
Passwords	23
Choosing the method for adding the storage array to the management domain	24
Configuring management port IP addresses using the Quick Connect utility	25
Using automatic discovery to add storage arrays to the management domain	25
Manually configuring the controllers by setting up a temporary private network	26
Configuring management port using System Manager	27
Configuring a management port using Storage Manager	29
Configuring multipath	31
Overview of multipath drivers	31
Multipath driver setup considerations	31
Supported multipath drivers	32
Automatic Load Balancing feature overview	32
Multipath configuration diagrams	33
How a multipath driver responds to a data path failure	36
User responses to a data path failure	36
Power methods for configuring multipath	37
Dividing I/O activity between two RAID controllers to obtain the best performance	37
Upgrading VMware to a release supported with SANtricity 11.30	38

Configuring virtualization and clustering	40
Virtualization considerations	40
Multipathing and virtualization	41
Host clustering support	41
Cluster accessibility	41
Cluster topology	42
Cluster shared storage in SANtricity	43
What are SCSI reservations?	43
Deciding whether to use disk pools or volume groups	44
Creating a volume group	44
Creating a volume group using the AMW	47
Storage partitions	48
Copyright information	52
Trademark information	53
How to send comments about documentation and receive update notifications	54

Deciding whether to use this Power Guide

You can customize the installation and configuration of the management software and E-Series storage array to fit your data storage requirements. The quickest path is described in the SANtricity Express Guide for your operating system. This Power Guide provides additional options beyond those included in the Express Guides. You can use a mixture of express methods and power methods to customize your installation.

Use this document for one of the following reasons:

You have...	...and you want to...
Planned for an express installation of SANtricity Storage Manager or an express configuration of SANtricity System Manager on your operating system	<ol style="list-style-type: none"> 1. Review the options for managing your storage array by exploring the table of contents of the Express Guide and this Power Guide. 2. Verify your decisions by using the Configuration worksheet on page 10. 3. Proceed through the Express Guide for your operating system. Review the options in this Power Guide and choose the variations you want to consider for your storage installation.
Completed an express method install using one of the E-Series Express Guides	Review the options for managing your storage arrays. See Configuration options on page 6.
An active E-Series configuration	Consider adding options or modifying your installation: <ol style="list-style-type: none"> 1. Verify your decisions by using the Configuration worksheet on page 10. 2. Read the conceptual information and optional procedures in this Power Guide. 3. Follow the procedures that are appropriate for your data storage requirements.

Related information

[NetApp E-Series Systems Documentation Center](#)

Configuration options

When planning the installation of an E-Series storage array, you can consider a number of options beyond the express method, including how to install the storage management software, how to manage the domain, and how to configure AutoSupport and alerts.

Type of storage array

If you have E-Series storage arrays, you could have one or more of these models:

- E5700
- E2800
- E5600
- E2700

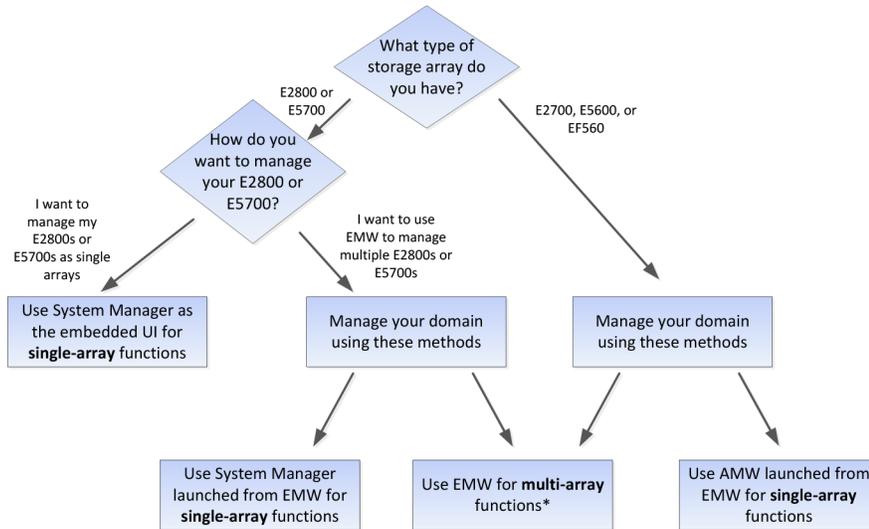
Your options for storage management software vary depending on the array type.

Storage management software

NetApp's two software interfaces, SANtricity **Storage** Manager and SANtricity **System** Manager, are each appropriate in specific use cases:

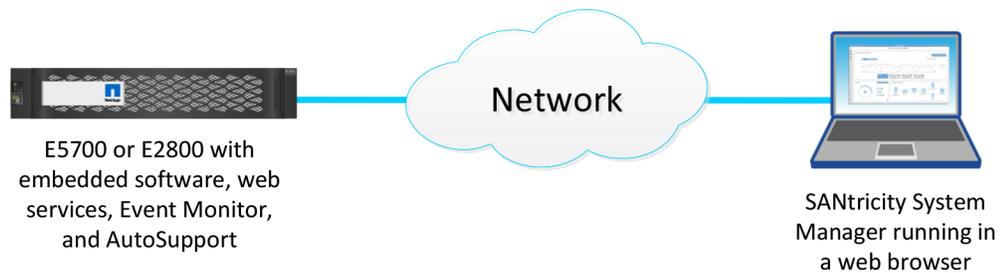
- SANtricity Storage Manager is compatible with the E2700 and E5600 storage arrays. SANtricity Storage Manager's client-based user interface has an **Enterprise Management Window (EMW)** and an **Array Management Window (AMW)**.
 - The EMW provides functions for configuring and managing multiple arrays.
 - The AMW provides functions for configuring and managing a single array. You launch the AMW from within the EMW.
- SANtricity System Manager's browser-based user interface is appropriate for managing either single or multiple E2800 or E5700 arrays. How you launch SANtricity Storage Manager depends on whether you want to manage a single array or multiple arrays.
 - To manage one or more E2800 or E5700 arrays as single arrays, launch System Manager in a browser.
 - To manage one or more E2800 or E5700 arrays as a multiple-array configuration, launch System Manager from the EMW.

Use the following decision tree to help you determine which storage management software you will use.

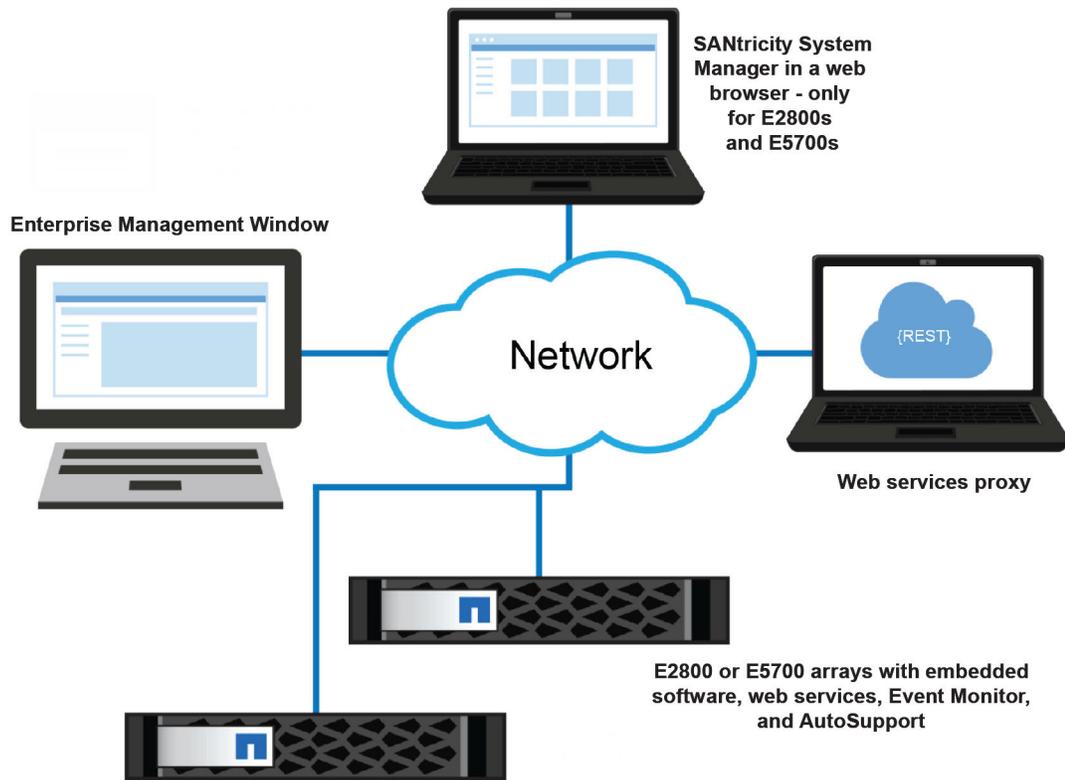


The following configuration examples further illustrate the use of the appropriate storage management software.

- **Single E2800 or E5700 storage array** — If you have a single E2800 or E5700 array and are not using either the Synchronous Mirroring or Asynchronous Mirroring feature, all configuration can be handled from SANtricity System Manager. .



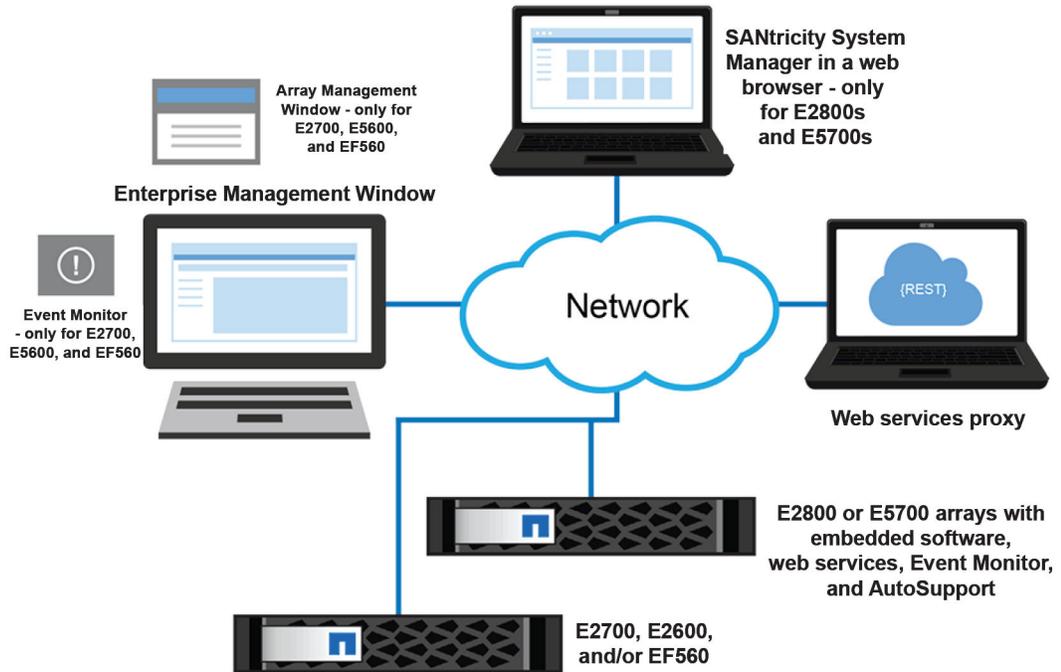
- **Multiple E2800 or E5700 storage arrays** — If you have more than one E2800 or E5700 storage array, you can install the EMW to manage your storage environment while handling storage array-based configuration through SANtricity System Manager. The EMW is included with SANtricity Storage Manager.



Note: If you are not using Synchronous or Asynchronous Mirroring features, you do not need to install the EMW. Instead, you can bookmark multiple SANtricity System Manager storage arrays in a browser.

- **Mixed array environment** — You must use the EMW that is part of the SANtricity Storage Manager installation if either of the following statements is true:
 - You have one or more E2800 storage arrays and any E2700, E5600, or EF560 storage arrays and want to have the E2800 or E5700 storage array included in your aggregate view.
 - You want to use Synchronous or Asynchronous Mirroring.

For array-based tasks on the E2800 or E5700 storage arrays, use SANtricity System Manager launched from the EMW. For array-based tasks on E2700, E5600, or EF560 storage arrays, use the AMW launched from the EMW.



AutoSupport and alerts

You configure AutoSupport (ASUP), email, and syslog alerts differently, depending on the type of storage array:

- **E2800, E5700** — You must configure AutoSupport and alerts on each storage array. These components are embedded in the E2800 and E5700 controllers.
- **E2700, E5600, and EF560** — You can configure AutoSupport and alerts globally by using the EMW.

Related information

[SANtricity Storage Manager 11.40 Installing and Configuring for VMware Express Guide](#)

[SANtricity System Manager 11.40 Installing and Configuring for VMware Express Guide](#)

Configuration worksheet

The storage configuration worksheet allows you to track your decisions about your E-Series configuration. Express methods and power methods are listed.

Circle your components and options in the table. For express method instructions, see the Express Guide for your operating system (OS).

Decision/Component	Express method	Power method (described in this Power Guide)
Controller model	<ul style="list-style-type: none"> • E5700 • E2800 • E2700 • E5600 • EF560 	<ul style="list-style-type: none"> • E5700 • E2800 • E2700 • E5600 • EF560 <p>See Configuration options on page 6.</p>
Storage management method (physical connectivity)	Out-of-band	In-band See Deciding on the management method on page 12.
<p>Management software components</p> <p>You use SANtricity Storage Manager or SANtricity System Manager for different storage arrays and different purposes. See Configuration options on page 6.</p>	<ul style="list-style-type: none"> • SANtricity Storage Manager <ul style="list-style-type: none"> ◦ Enterprise Management Window (EMW) ◦ Array Management Window (AMW) ◦ CLI ◦ Event Monitor • SANtricity System Manager <ul style="list-style-type: none"> ◦ For E2800 or E5700 controller shelves ◦ Not a separate installation ◦ Browser-based • Multipath driver • Unified Host Utilities 	<ul style="list-style-type: none"> • SMagent (part of the host manager installation) • Multipath driver • Other utilities, such as SMdevices <p>See Deciding which packages to install on page 17.</p>
Using the storage array as a boot device	No	Yes See Installing the storage array as a boot device on page 16.

Decision/Component	Express method	Power method (described in this Power Guide)
Using Silent Mode when installing SANtricity Storage Manager	No	Yes See <i>Installing SANtricity Storage Manager packages using silent mode</i> on page 17.
I/O protocol	All protocol-specific tasks are described in Express Guides	No additional protocol-specific options.
Management IP addressing method	Static IP, using Quick Connect utility	<ul style="list-style-type: none"> • Static IP, by temporarily setting up a private network • Dynamic host configuration protocol (DHCP) • IPv6 stateless address auto configuration See <i>Setting IP addresses</i> on page 21 and <i>Choosing the method for adding the storage array to the management domain</i> on page 24.
Disk pools (pools) or volume groups	Disk pools (pools)	Disk pools (pools) or volume groups See <i>Deciding whether to use disk pools or volume groups</i> on page 44.

Related references

Configuration options on page 6

Deciding on the management method

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

Management methods

You can choose the best management method based on your system configuration and management goals. You manage a storage array from a management station or from a host.

Management methods include:

- Out-of-band management
- In-band management
- A combination of out-of-band and in-band management

Storage management includes these activities:

- Configuring available storage array capacity to maximize data availability, optimize application performance, and make the most of storage resources
- Configuring destinations to receive alert messages for critical problems concerning one or more storage arrays
- Monitoring storage arrays for problems or conditions that require attention
- Recovering from storage array problems to maximize data availability

Note: In-band management for VMware systems is supported only when using a Virtual Machine hosted on a VMware host. For more details, refer to [Out-of-band and in-band requirements](#) on page 12.

Out-of-band and in-band requirements

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

Management method	Requirements	Advantages	Disadvantages
All out-of-band methods	Connect separate Ethernet cables to each controller.	<p>This method does not use I/O path bandwidth for storage array management functions.</p> <p>This method does not use the SAS, Fibre Channel or iSCSI bandwidth for storage array management functions.</p>	<p>Ethernet cables are required.</p> <p>Does not allow you to choose which controller is used for the EMW. Controller A is used until SANtricity Storage Manager has difficulty communicating on that path. Then the system switches to controller B.</p>

Management method	Requirements	Advantages	Disadvantages
Out-of-band <i>without</i> a DHCP server	Manually configure the network settings on the controllers.	--	You must manually configure the network settings on the controllers.
Out-of-band – IPv6 stateless address auto-configuration <i>without</i> a DHCP server (IPv6 networks only)	<p>Connect at least one router for sending the IPv6 network address prefix in the form of router advertisements.</p> <p>The router is necessary to route the IPv6 packets outside the local network.</p>	<p>No additional manual network configuration is required on the controllers.</p> <p>By default, the controllers automatically obtain their IP addresses by combining the auto-generated link local address and the IPv6 network address prefix after you turn on the power to the controller-drive tray.</p>	A router is required.

Management method	Requirements	Advantages	Disadvantages
<p>Out-of-band <i>with</i> a DHCP server (IPv4 networks only)</p>	<p>Connect separate Ethernet cables to each controller.</p> <p>Assign either static IP addresses or dynamic IP addresses to the controllers using your DHCP server. Alternatively, both the SANtricity System Manager and the SANtricity Storage Manager AMW can be used to set the IP addresses after the storage array has been discovered. It is recommended that you 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.</p> <p>Check your DHCP server for the IP addresses that are associated with the media access control (MAC) addresses of the controllers.</p> <p>The MAC address appears on a label on each controller in the form: <i>xx.xx.xx.xx.xx.xx</i> .</p> <div data-bbox="483 1192 863 1289" style="border: 1px solid black; padding: 5px; text-align: center;">  <p>00.A0.B8.00.00.00 00.A0.B8.00.00.00</p> <p>1T12345678 1T12345678</p> </div>	<p>No additional manual network configuration is required on the controllers.</p> <p>By default, the controllers automatically obtain their IP addresses from the DHCP server after you turn on the power to the controller-drive tray.</p> <p>This method does not use a special Access Volume to communicate with the host.</p>	<p>No additional disadvantages.</p>

Management method	Requirements	Advantages	Disadvantages
In-band	<p>For VMware, you must use a Virtual Machine that is hosted on a VMware host. The SMagent is installed on the Virtual Machine, which could be either a Linux or Windows Guest OS.</p> <p>The in-band method requires a special access volume that must be assigned or mapped to either LUN 7 or 31 to communicate between the management station and the storage array. This volume is created automatically. On the ESXi host, this access volume would be a physical Raw Disk Mapping (RDM) to the Virtual Machine that is running SMagent to access the storage array in-band.</p> <p>If a firewall is installed on the hosted Virtual Machine, ensure that port 2463 is open.</p>	No additional manual network configuration is required on the controller.	<p>This method:</p> <ul style="list-style-type: none"> • Uses both a LUN on the host and the SAS, Fibre Channel, or iSCSI bandwidth for storage array management functions. • Is not supported on System Manager; you must use the CLI. • Does not allow you to choose which controller is used for the command-line interface (SMcli).

Installing SANtricity Storage Manager

If the express method of installing SANtricity Storage Manager does not meet the requirements of your configuration, you can consider alternate power methods. These methods apply to Storage Manager only, and not System Manager. System Manager is embedded in the controller, so you do not need to install it.

Related information

[SANtricity Storage Manager 11.40 Installing and Configuring for VMware Express Guide](#)

[SANtricity System Manager 11.40 Installing and Configuring for VMware Express Guide](#)

Installing the storage array as a boot device

Before you install the storage management software components on the host, you must prepare the storage array and the host. Because E-Series storage behaves as a block device, you can install an operating system on it and boot that operating system from an E-Series storage array, instead of relying on local storage.

Using the E-Series storage array as a boot device serves as a less expensive, potentially faster alternative to internal storage. For example, if operating a Blade system, this process is much less expensive than purchasing internal storage for all blades. This process is called SAN booting - or relying on the SAN to boot a host. The concept of SAN boot is straight forward; however, the execution can become complicated.

The following describes the overall workflow required for setting up a SAN boot on E-Series storage:

- The host, and more specifically the adapter attached to E-Series storage, is directed to present a mapped or assigned volume from storage prior to boot (in BIOS, uEFI, or another appropriate type of firmware).
This process is vendor-specific, protocol-specific, and architecture specific.
- The host can boot using the installation media.
- The installation selects the volume provided by storage to install.
Sometimes this requires a driver update disk (DUD). Additionally, failover might or might not have to be loaded during this step, depending on the operating system.
- After reboot, the boot options must set the newly-installed volume as the primary boot option.
This step is vendor-specific for the adapter as well as the server.

Note: NetApp recommends using LUN 0 for booting, and some operating systems might require it.

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. For example, Fibre Channel and SAS connections are supported, while iSER over Infiniband, SRP over InfiniBand and some iSCSI connections are not supported.

The following table shows which operating systems support this configuration, but you should consult the [Interoperability Matrix Tool](#) to ensure that your HBA and operating system are supported.

Operating system	Boot device support	Recommended number of paths for installation
AIX	Yes, where supported by the HBAs	2
HP-UX	Yes, where supported by the HBAs	2
Linux	Yes, where supported by the HBAs	2
Mac OS X	No	1
Solaris	Yes, where supported by the HBAs	2
VMware	Yes, where supported by the HBAs	2
Windows	Yes, where supported by the HBAs	1 (works with 2, but 1 is recommended)

Installing SANtricity Storage Manager packages using silent mode

You can use the Silent installation mode for any OS that is supported by Install. Silent mode requires minimal user interactions and is useful when deploying a large number of servers that are not connected to terminals.

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:

This command creates the `installer.properties`.

Deciding which packages to install

Different storage management software components and packages are required for different machines. Additionally, you will install different components depending on the environment you need to support for your particular configuration.

Host operating systems

Considerations for both SANtricity System Manager and 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.

SANtricity Storage Manager or SANtricity System Manager?

To configure and manage E2700 or E5600 storage arrays, you use SANtricity Storage Manager's Array Management Window (AMW) and Enterprise Management Window (EMW). If you have an

E2800 or E5700 storage array, you configure it using the browser-based SANtricity System Manager rather than through SANtricity Storage Manager's AMW. If you have multiple types of storage arrays or more than one E2800 or E5700 and want to manage your entire environment, you install and use SANtricity Storage Manager's EMW.

SANtricity System Manager is browser-based, so there is no installation required. After you install your E2800 or E5700 hardware and connect it to the network by assigning appropriate IPs, subnet masks, and the gateway for the controllers, you access SANtricity System Manager by pointing a browser to the E2800 or E5700's IP address or domain name.

SANtricity Storage Manager components

Client

This package contains both the graphical user interface (GUI) (containing both the EMW and the AMW) and the command line interface (CLI) for managing the storage arrays. This package also contains the Event Monitor that sends alerts when a critical problem exists with the storage array.

Multipath driver

For this operating system, the preferred multipath driver is included "in-box" and is not available from the SANtricity host install package. The multipath driver 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. Always check the [Interoperability Matrix Tool](#) to verify what multipath drivers are supported for your configuration.

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.

Event Monitor

During the client installation, you might be asked whether you want to start the Event Monitor.

If you are running an E2800 or E5700 storage array, the Event Monitor resides on the controller and must be configured for each storage array. Use either SANtricity System Manager or the SMcli to complete the configuration task.

If you have an E2700 or E5600 storage array, start the monitor on only one management station that runs continuously. If you start the monitor on more than one management station, you receive duplicate alert notifications about problems with the storage array. If you install SANtricity components on more than one management station and are not asked about the Event Monitor, verify that the monitor is active on only one of the systems.

Note: To receive critical alert notifications and to access the AutoSupport (ASUP) feature with E2700 or E5600 storage arrays, you must have Event Monitor running on just one management station. With the E2800 or E5700 storage array, AutoSupport functionality is embedded in the controller.

Related information

[SANtricity System Manager 11.40 Installing and Configuring for VMware Express Guide](#)

Installing the SANtricity software on hosts, monitors, and management stations

You can use the following software configuration diagrams and accompanying tables to determine which software packages to install on each machine (host, monitor, or management station):

For this operating system, the preferred multipath driver is included "in-box" and is not available from the SANtricity host install package

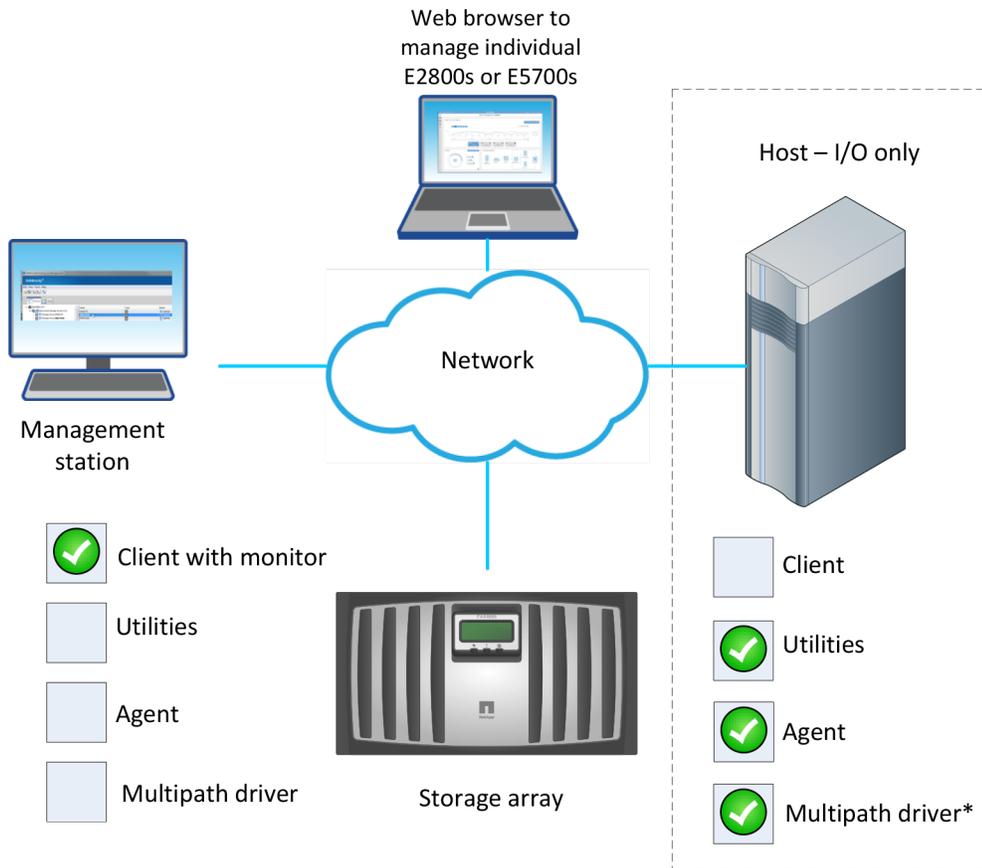
The following table shows the packages that apply to particular installations.

Installation wizard selections	
Type of installation	Client
Management Station	✓

Installing on the management station

The following conceptual diagram and table provide basic information for installing on the management station for VMware.

Note: In a VMware environment, the management station is typically a Windows management station.



Machines and required software: Host (I/O only)		
Minimum Software Required	Installation Package (Choose One) (See the Installation wizard selections table above.)	Notes
n/a	Client	
The preferred Multipath driver is "in-box" with the operating system for VMware systems.		

Adding the storage array to the management domain

Before you add the storage array to the management domain, review the guidelines and complete the preliminary tasks. Then, choose from a list of methods for adding the storage array.

Preparing to add the storage array to the management domain

You must prepare the storage array before adding it to the management domain, which consists of discovering any storage array within the local sub-network so that they display within the EMW.

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

If the express method of using the Quick Connect utility to assign static IP addresses does not meet the requirements of your configuration, you can use one of the alternate methods for configuring IP addresses.

By default, E-Series controllers ship with DHCP enabled on both network ports. You can assign static IP addresses, use the default static IP addresses, or use DHCP-assigned IP addresses. You can also use IPv6 stateless auto-configuration.

Note: IPv6 is disabled by default on new E-Series systems, but you can configure the management port IP addresses using an alternate method, and then enable IPv6 on the management ports using SANtricity System Manager.

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 might 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 for E2800 and E5700 controllers, use SANtricity System Manager. To set static IP addresses for E2700 and E5600 controllers, 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.

Related concepts

[Choosing the method for adding the storage array to the management domain](#) on page 24

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.”

Passwords

Access Management, new in the 11.40 release, requires that users log in to SANtricity System Manager with assigned login credentials. Each user login is associated with a user profile that includes specific roles and access permissions. If you do not want to use Access Management, or if you have an E2700 or E5600 storage array for which the feature is unsupported, you can configure each storage array with an Administrator password. An optional Monitor password is available for E2700 and E5600 arrays.

Administrators can implement Access Management using one or both of these methods:

- Using RBAC (role-based access control) capabilities enforced in the storage array, which includes pre-defined users and roles.
- Connecting to an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory, and then mapping the LDAP users to the storage array's embedded roles.

If you do not use Access Management or it is not supported, 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.

Note that a Monitor password is not supported with SANtricity System Manager.

On SANtricity System Manager, you are asked if you want to set an Administrator password during initial set up.

On SANtricity Storage Manager, you are 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.

Choosing the method for 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.

There are three primary methods of configuring the management ports of a storage array and adding them to the management domain:

- **Static IP addressing** - An Internet Protocol (IP) address for each management port that you enter. These addresses are typically assigned by a network administrator.
- **DHCP addressing** - An Internet Protocol (IP) address that the Dynamic Host Configuration Protocol (DHCP) server assigns. DHCP provides three mechanisms for IP address allocation. Automatic allocation is defined as DHCP assigning a permanent IP address to a client. Dynamic allocation is defined as DHCP assigning an IP address to a client for a limited time period or until the client explicitly lets go of the address. Manual allocation is defined as the network administrator assigning the IP address of the client, and DHCP conveys the assigned address to the client. A network uses one or more of these mechanisms, depending on the policies that the network administrator specifies.
- **Stateless address autoconfiguration with IPv6** - With stateless auto-configuration, hosts do not obtain addresses and other configuration information from a server. Stateless auto-configuration in IPv6 features link-local addresses, multicasting, and the Neighbor Discovery (ND) protocol. IPv6 can generate the interface ID of an address from the underlying data link layer address.

Note: You can change the configuration of a storage array to use a different type of management port IP addressing at any time. See the SANtricity System Manager online help or the SANtricity Storage Manager online help for detailed procedures.

Use one of the following methods to connect your E-Series storage arrays to the management domain:

If you are using...	...do this...
Static IP addressing	Use the Quick Connect utility. See Configuring IP addresses using the Quick Connect utility on page 25.
DHCP addressing of the management ports	Use auto-discovery to discover your storage array. See Using automatic discovery to add storage arrays to the management domain on page 25.
Stateless address auto-configuration, no DHCP server	Note: For E2700 and E5600 arrays only, the management station must reside on the same subnetwork as the array during controller management IP configuration.
Static IP addressing, and need an alternative to using the Quick Connect Utility	Temporarily set up a private network to configure the management ports. Note: For E2700 and E5600 arrays only, 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 26.

Related information

[SANtricity Storage Manager 11.40 Installing and Configuring for VMware Express Guide](#)
[SANtricity System Manager 11.40 Installing and Configuring for VMware Express Guide](#)

Configuring management port IP addresses using the Quick Connect utility

In this best-practices method for configuring communications, you configure the management station and array controllers to communicate using the Quick Connect utility.

Before you begin

- 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).

About this task

The following figures show the location of management port 1 on the controllers.

Steps

1. Go to [SANtricity Quick Connect](#). Download and install the utility.
2. Follow the directions on the Wizard screens to configure your management port and to configure the IP address of each controller.
3. Connect an Ethernet cable to management port 1 (labeled P1) on each controller, and connect the other end to your network.

Note: Do not use port 2 on either controller. These ports are reserved for use by NetApp technical personnel.

Using automatic discovery to add storage arrays to the management domain

You can use automatic discovery to set the controller IP addresses using 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.

About this task

This procedure specifically applies to users with SANtricity Storage Manager configurations. If you have a SANtricity System Manager configuration, refer to [Configuring management port using System Manager](#) on page 27.

Steps

1. Open **SANtricity Storage Manager**.

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

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. 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.

Manually configuring the controllers by setting up a temporary private network

You can manually configure the IP addresses on the controllers by setting up a temporary private network.

Before you begin

- 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 A.

Note: Do not use port 2 on either controller. These ports are reserved for use by NetApp technical personnel.

- 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 shelves 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 A IP to make sure it is accessible.

Example

```
> 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. Change the networking configuration.

The procedure you use depends on the model number of your storage array.

- For E2800 and E5700 storage arrays, see [Configuring a management port using System Manager](#) on page 27.
 - For E2700 and E5600 storage arrays, see [Configuring a management port using SANtricity Storage Manager](#) on page 29.
3. Disconnect the Ethernet cable from your management station, and reconnect the Ethernet cables from the controllers into your regular network.
 4. Complete the steps necessary to change the management station's IP address back to what it was initially.

Configuring management port using System Manager

The controller includes an Ethernet port used for system management. If necessary, you can change its transmission parameters and IP addresses.

About this task

During this procedure, you select port 1 and then determine the speed and port addressing method. Port 1 connects to the network where the management client can access the controller and System Manager.

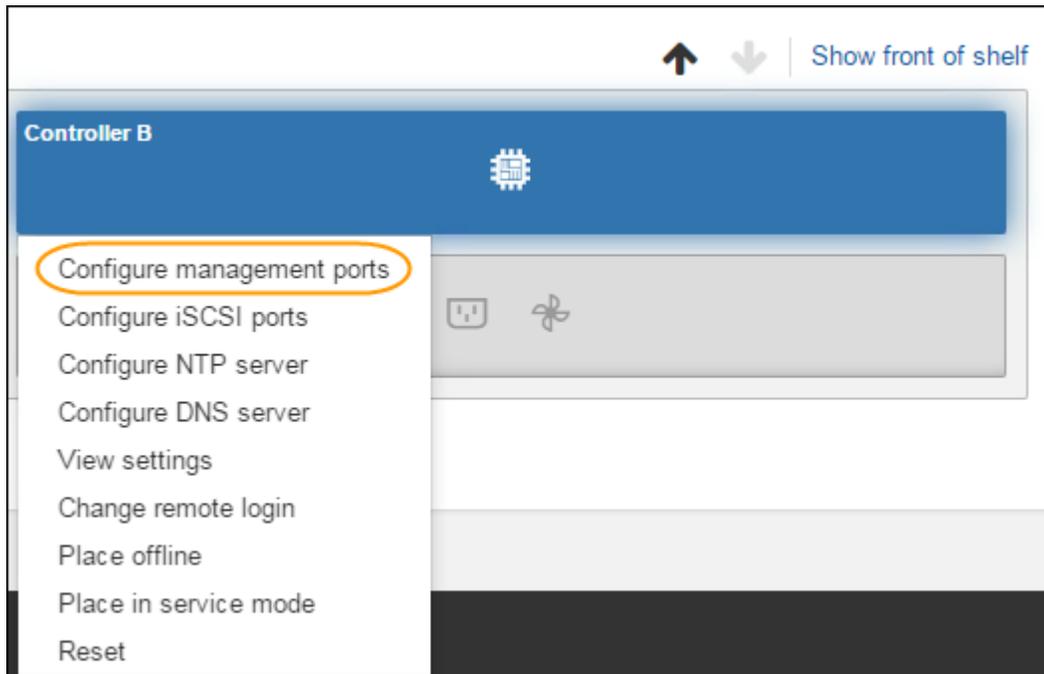
Note: Do not use port 2 on either controller. Port 2 is reserved for use by technical support.

Steps

1. Select **Hardware**.
2. If the graphic shows the drives, click **Show back of shelf**.
The graphic changes to show the controllers instead of the drives.
3. Click the controller with the management port you want to configure.

The controller's context menu appears.

4. Select **Configure management ports**.



The Configure Management Ports dialog box opens.

5. Make sure port 1 is displayed, and then click **Next**.
6. Select the configuration port settings, and then click **Next**.

Field Details

Field	Description
Speed and duplex mode	Keep the Auto-negotiate setting if you want System Manager to determine the transmission parameters between the storage array and the network; or if you know the speed and mode of your network, select the parameters from the drop-down list. Only the valid speed and duplex combinations appear in the list.
Enable IPv4 / Enable IPv6	Select one or both options to enable support for IPv4 and IPv6 networks.

If you select **Enable IPv4**, a dialog box opens for selecting IPv4 settings after you click **Next**. If you select **Enable IPv6**, a dialog box opens for selecting IPv6 settings after you click **Next**. If you select both options, the dialog box for IPv4 settings opens first, and then after you click **Next**, the dialog box for IPv6 settings opens.

7. Configure the IPv4 and/or IPv6 settings, either automatically or manually.

Field Details

Field	Description
Automatically obtain configuration from DHCP server	Select this option to obtain the configuration automatically.

Field	Description
Manually specify static configuration	<p>Select this option, and then enter the controller's IP address. (If desired, you can cut and paste addresses into the fields.) For IPv4, include the network subnet mask and gateway. For IPv6, include the routable IP address and router IP address.</p> <p>Attention: If you change the IP address configuration, you lose the management path to the storage array. Using the SANtricity Storage Manager Enterprise Management Window (EMW), you must remove the device from the EMW. Add it back to the EMW by selecting Edit > Add Storage Array, and then enter the new IP address. For more information, refer to the online help topics in the EMW.</p>

- Click **Finish**.

Result

The management port configuration is displayed in the controller settings, Management Ports tab.

Configuring a management port using Storage Manager

Steps

- Open the **SANtricity Storage Manager**.

The **Enterprise Management Window (EMW)** is displayed.
- 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.
- Name the storage array.
 - In the **EMW Setup** tab, select **Name/Rename Storage Arrays**.
 - In the **Select storage array** list, select the storage array you added.
 - 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.
 - Select **OK**.
- Configure the network configuration information of the controllers, using information you obtain from your network administrator.
 - In the AMW, select the **Hardware** tab.
 - Select **Hardware > Controller > Configure > Management Ports**.
 - On the **Change Network Configuration** dialog box, select Controller A, Port 1 in the **Ethernet port** drop-down list.
 - 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. In the **Ethernet port** drop-down list, select Controller B, Port 1, and repeat step c through step f for controller B.
- h. Select **OK**.

Configuring multipath

If the express method for configuring the multipath driver does not meet the requirements of your configuration, you can consider alternate power methods.

Related concepts

[Power methods for configuring multipath](#) on page 37

[Configuring virtualization and clustering](#) on page 40

Related information

[SANtricity Storage Manager 11.40 Installing and Configuring for VMware Express Guide](#)

[SANtricity System Manager 11.40 Installing and Configuring for VMware Express Guide](#)

Overview of multipath drivers

Multipath drivers help the hosts continue to operate without interruption when a physical path fails.

Multipath drivers provide a redundant path for the data cables connecting the storage array's controllers to the host bus adapters. For example, you can connect two host bus adapters to the redundant controller pair in a storage array, with different data cables for each controller. If one host bus adapter, one data cable, or one controller fails, the multipath driver automatically reroutes input/output (I/O) to the good path.

Multipath drivers provide these functions:

- They automatically identify redundant I/O paths.
- They automatically reroute I/O to an alternate controller when a controller fails or all of the data paths to a controller fail (failover).
- They check the state of known paths to the storage array.
- They provide status information on the controller and the bus.
- They check to see if Service mode is enabled on a controller and if the asymmetric logical unit access (ALUA) mode of operation has changed.
- They provide load balancing between available paths.

Multipath driver setup considerations

Most storage arrays contain two controllers that are set up as redundant controllers. If one controller fails, the other controller in the pair takes over the functions of the failed controller, and the storage array continues to process data. You can then replace the failed controller and resume normal operation. You do not need to shut down the storage array to perform this task.

The redundant controller feature is managed by the multipath driver software, which controls data flow to the controller pairs. This software tracks the current status of the connections and can perform the switch-over.

Whether your storage arrays have the redundant controller feature depends on a number of items:

- Whether the hardware supports it. Check to see whether you have duplex or simplex controllers in your configuration.

- Whether your OS supports certain multipath drivers. Refer to the installation and support guide for your operating system to determine whether your operating system supports redundant controllers.
- How the storage arrays are connected.

With the ALUA (I/O Shipping) feature, a storage array can service I/O requests through either controller in a duplex configuration; however, I/O shipping alone does not guarantee that I/O is routed to the optimized path.

Supported multipath drivers

E-Series storage arrays support multipath drivers specific to your operating system and a recommended host type.

This table provides general guidelines. Refer to the [Interoperability Matrix Tool](#) for compatibility information for specific HBA, multipath driver, OS level, and controller-drive tray support.

Operating System	Multipath driver	Recommended host type
VMware	Native Multipathing Plugin (NMP) with VMW_SATP_ALUA Storage Array Type Plugin (SATP)	VMware

The preferred multipath driver is provided "in-box" with the operating system.

You must manually set the host type in SANtricity Storage Manager.

- To manually set the host type, from the Array Management Window, select the **Host Mappings** tab, select the host, and then select **Host Mappings > Host > Change Host Operating System**.
- If you are using SANtricity Storage Manager but not using partitions (for example, no Hosts defined), set the appropriate host type for the Default Group by selecting **Host Mappings > Default Group > Change Default Host Operating System**.
- If you are using SANtricity System Manager, use the "Create host manually" procedure in the System Storage Manager online help.

Automatic Load Balancing feature overview

The Automatic Load Balancing feature provides automated I/O workload balancing and ensures that incoming I/O traffic from the hosts is dynamically managed and balanced across both controllers.

What is Automatic Load Balancing?

The Automatic Load Balancing feature provides improved I/O resource management by reacting dynamically to load changes over time and automatically adjusting volume controller ownership to correct any load imbalance issues when workloads shift across the controllers.

The workload of each controller is continually monitored and, with cooperation from the multipath drivers installed on the hosts, can be automatically brought into balance whenever necessary. When workload is automatically re-balanced across the controllers, the storage administrator is relieved of the burden of manually adjusting volume controller ownership to accommodate load changes on the storage array.

When Automatic Load Balancing is enabled, it performs the following functions:

- Automatically monitors and balances controller resource utilization.
- Automatically adjusts volume controller ownership when needed, thereby optimizing I/O bandwidth between the hosts and the storage array.

Host types that support the Automatic Load Balancing feature

Even though Automatic Load Balancing is enabled at the storage array level, the host type you select for a host or host cluster has a direct influence on how the feature operates. When balancing the storage array's workload across controllers, the Automatic Load Balancing feature attempts to move volumes that are accessible by both controllers and that are mapped only to a host or host cluster capable of supporting the Automatic Load Balancing feature. This behavior prevents a host from losing access to a volume due to the load balancing process; however, the presence of volumes mapped to hosts that do not support Automatic Load Balancing affects the storage array's ability to balance workload. For Automatic Load Balancing to balance the workload, the multipath driver must support TPGS and the host type must be included in the following table.

Host type supporting Automatic Load Balancing	With this multipath driver
Windows or Windows Clustered	MPIO with NetApp E-Series DSM
Linux DM-MP (Kernel 3.10 or later)	DM-MP with <code>scsi_dh_alua</code> device handler
VMware	Native Multipathing Plugin (NMP) with <code>VMW_SATP_ALUA</code> Storage Array Type plug-in

Note: With minor exceptions, host types that do not support Automatic Load Balancing continue to operate normally whether or not the feature is enabled. One exception is that if a system has a failover, storage arrays move unmapped or unassigned volumes back to the owning controller when the data path returns. Any volumes that are mapped or assigned to non-Automatic Load Balancing hosts are not moved.

See the [Interoperability Matrix Tool](#) for compatibility information for specific multipath driver, OS level, and controller-drive tray support.

Note: For a host cluster to be considered capable of Automatic Load Balancing, all hosts in that group must be capable of supporting Automatic Load Balancing.

Multipath configuration diagrams

You can configure multipath in several ways. Each configuration has its own advantages and disadvantages.

This section describes the following configurations:

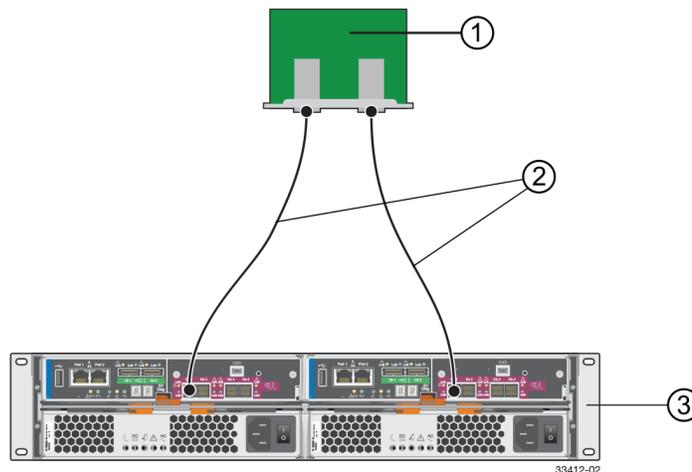
- Single-host configuration
- Direct connect and fabric connect configurations

This section also describes how the storage management software supports redundant controllers.

Single-Host configuration

In a single-host configuration, the host system contains two host bus adapters (HBAs), with a port on each HBA connected to different controllers in the storage array. The storage management software is installed on the host. The two connections are required for maximum failover support for redundant controllers.

Although you can have a single controller in a storage array or a host that has only one HBA port, you do not have complete failover data path protection with either of those configurations. The cable and the HBA become a single point of failure, and any data path failure could result in unpredictable effects on the host system. For the greatest level of I/O protection, provide each controller in a storage array with its own connection to a separate HBA in the host system.



1. Host System with Two SAS, Fibre Channel, iSCSI, or InfiniBand Host Bus Adapters
2. SAS, Fibre Channel, iSCSI, iSER over Infiniband or SRP over InfiniBand Connection – The Network Protocol Connection Might Contain One or More Switches
3. Storage Array with Two Controllers

Direct connect and fabric connect configurations

In a direct connect or fabric connect configuration, two host systems are each connected by two connections to both of the controllers in a storage array. SANtricity Storage Manager, including multipath driver support, is installed on each host.

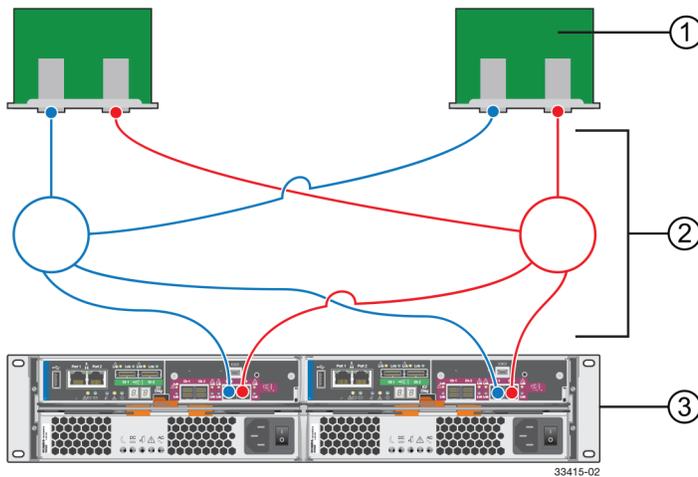
Not every operating system supports this configuration. Consult the restrictions in the installation and support guide specific to your operating system for more information. Also, the host systems must be able to handle the multi-host configuration. Refer to the applicable hardware documentation.

Neither SANtricity Storage Manager nor SANtricity System Manager cannot be installed on VMware Hosts, as VMware only supports the native multipath driver.

In either a direct connect or fabric connect configuration, each host has visibility to both controllers, all data connections, and all configured volumes in a storage array.

The following conditions apply to these both direct connect and fabric connect configurations:

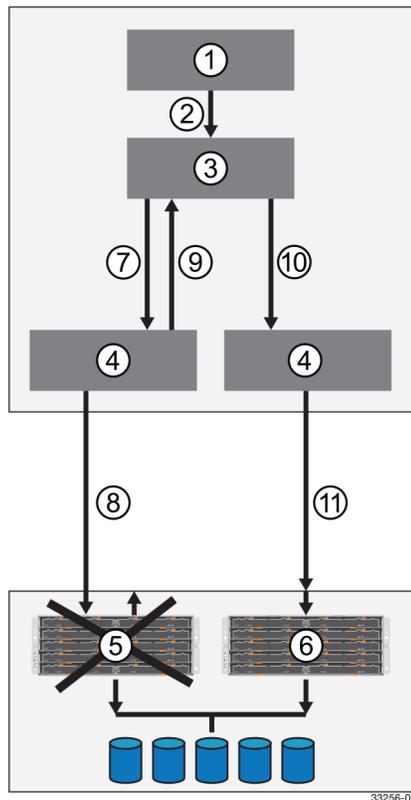
- Both hosts must have the same operating system version installed.
 - Note:** For VMware, this condition does not apply because you can cluster ESXi 5.0, 5.1, 5.5, and 6.0 releases together.
- The multipath driver configuration might require tuning.
- A host system might have a specified volume or volume group reserved, which means that only that host system can perform operations on the reserved volume or volume group.



1. Two Host Systems, Each with Two SAS, Fibre Channel, or iSCSI Host Bus Adapters
2. SAS, Fibre Channel, or iSCSI Connections with Two Switches (Might Contain Different Switch Configurations)
3. Storage Array with Two Controllers

Supporting redundant controllers

The following figure shows how multipath drivers provide redundancy when the host application generates a request for I/O to controller A, but controller A fails. Use the numbered information to trace the I/O data path.



1. Host Application
2. I/O Request
3. Multipath Driver
4. Host Bus Adapters
5. Controller A Failure
6. Controller B
7. Initial Request to the HBA
8. Initial Request to the Controller Failed
9. Request Returns to the Multipath Driver
10. Failover Occurs and I/O Transfers to Another Controller
11. I/O Request Re-sent to Controller B

How a multipath driver responds to a data path failure

One of the primary functions of the multipath driver is to provide path management. Multipath drivers monitor the data path for devices that are not working correctly or for multiple link errors.

If a multipath driver detects either of these conditions, the failover driver automatically performs the following steps:

- The multipath driver checks for the redundant controller.
- The multipath driver performs a path failure if alternate paths to the same controller are available. If all of the paths to a controller are marked offline, the multipath driver performs a controller failure. The failover driver provides notification of an error through the OS error log facility.
- For multipath drivers that are not using ALUA drivers, the multipath driver transfers volume ownership to the other controller and routes all I/O to the remaining active controller.
- For ALUA-based multipath drivers, controller B redirects I/O to the surviving controller (controller B). Then, if controller A is still active, controller B ships the I/O to controller A (SAN path loss case). If controller A has failed, controller B triggers a forced ownership transfer from the failed controller to itself (controller B).

User responses to a data path failure

You can use the Major Event Log (MEL) to troubleshoot a data path failure.

The information in the MEL provides the answers to these questions:

- What is the source of the error?
- What is required to fix the error, such as replacement parts or diagnostics?

When troubleshooting, follow these guidelines:

- Under most circumstances, contact technical support any time a path fails and the storage array notifies you of the failure.
- Use the MEL to diagnose and fix the problem, if possible.
- If your controller has failed and your storage array has customer-replaceable controllers, replace the failed controller. Follow the instructions provided with the controller.

Power methods for configuring multipath

Depending on your requirements, such as dividing I/O activity between RAID controllers or handling compatibility and migration, you can use the power methods for configuring multipath drivers.

Dividing I/O activity between two RAID controllers to obtain the best performance

For the best performance of a redundant controller system, use the storage management software to divide I/O activity between the two RAID controllers in the storage array. You can use a graphical user interface (GUI) or the command line interface (CLI).

The Automatic Load Balancing feature enables the system to dynamically reassign ownership so it can optimize the bandwidth between the hosts and the storage array. Note the following guidelines:

- If the Automatic Load Balancing feature is enabled, you do not need to perform the management tasks described in this section.
- If Automatic Load Balancing is enabled, you can select a preferred owner for a new volume when it is created, because there is no load history on that volume yet.
- By default, whenever possible the multipath driver directs I/O at the controller that is the preferred owner. This default method applies whether either of the following is true:
 - Preferred ownership is assigned automatically (Automatic Load Balancing is enabled).
 - Preferred ownership is assigned manually (Automatic Load Balancing is disabled).
- If you choose to disable Automatic Load Balancing, perform the management tasks described in this section to divide I/O activity between the two RAID controllers in the storage array.

To use the GUI to divide I/O activity between two RAID controllers, perform one of these procedures:

- From the SANtricity Storage Manager Array Management Window:
 - **Specify the owner of the preferred controller of an existing volume** – Select **Volume > Change > Ownership/Preferred Path**.

Note: You also can use this method to change the preferred path and ownership of all volumes in a volume group at the same time.

- **Specify the owner of the preferred controller of a volume when you are creating the volume** – Select **Volume > Create**.

- From SANtricity System Manager:

Specify the owner of the preferred controller of an existing volume

1. Select **Storage > Volumes**.
2. Select any volume and then select **More > Change ownership**.

The **Change Volume Ownership** dialog box appears.

All volumes on the storage array appear in this dialog box.

3. Use the **Preferred Owner** drop-down list to change the preferred controller for each volume that you want to change, and confirm that you want to perform the operation.

- Using the CLI:

Go to the "Create RAID Volume (Free Extent Based Select)" online help topic for the command syntax and description.

Note: The volume might not use the new I/O path until the multipath driver reconfigures to recognize the new path. This action usually takes less than five minutes.

Upgrading VMware to a release supported with SANtricity 11.30

If upgrading from a VMware release not supported with SANtricity 11.30 to a VMware release supported with SANtricity 11.30 on the NetApp Interoperability Matrix Tool, neither SATP nor VAAI claim rule modifications are required. The claim rules are inbox for the following VMware releases: 5.5u3 and subsequent releases.

About this task

These can be verified by using the following esxcli command from the shell:

Steps

1. Verify that shell or remote SSH access is available to the ESXi host.
2. To verify the SATP claim rules, specify the following on the command line:

```
esxcli storage nmp satp rule list -s VMW_SATP_ALUA
```

The output should return the following:

Name	Vendor	Options	Rule Group
Claim Options	Default PSP	Description	
-----	-----	-----	-----
VMW_SATP_ALUA	NETAPP	reset_on_attempted_reserve	system
tpgs_on	VMW_PSP_RR	NetApp arrays with ALUA support	

3. **Note:** If the above output is not as listed, the consider checking the [Interoperability Matrix Tool](#) and ensuring that you are at the level supported by 11.30 SANtricity release.

to verify the core claim rules, specify the following on the command line:

```
esxcli storage core claimrule list -c Filter
```

The output should return the following:

Rule Class	Rule	Class	Type	Plugin
Matches	-----	-----	-----	-----
-----	-----	-----	-----	-----
Filter	65433	runtime	vendor	VAAI_FILTER
model=LUN*				vendor=NETAPP
Filter	65433	file	vendor	VAAI_FILTER
model=LUN*				vendor=NETAPP

Note: If the above output is not as listed, the consider checking the [Interoperability Matrix Tool](#) and ensuring that you are at the level supported by 11.30 SANtricity release.

4. To verify the VAAI claim rules, specify the following on the command line:

```
esxcli storage core claimrule list -c VAAI
```

The output should return the following:

```

Rule Class      Rule  Class      Type      Plugin
Matches
-----
VAAI           65433  runtime    vendor    VMW_VAAIP_NETAPP  vendor=NETAPP
model=LUN*
VAAI           65433  file       vendor    VMW_VAAIP_NETAPP  vendor=NETAPP
model=LUN*

```

Note: If the above output is not as listed, the consider checking the [Interoperability Matrix Tool](#) and ensuring that you are at the level supported by 11.30 SANtricity release.

5. Upgrade the controllers in the storage array to SANtricity OS software (controller software) 8.30 and the corresponding NVSRAM version.

Once finished upgrading to SANtricity OS software 8.30, the storage array automatically fails back.

6. From the host management client, verify that the host OS type is set to *VMWARE*. By default, the *VMWARE* host type enables both ALUA and TPGS.
7. You can enable the Automatic Load Balancing feature by doing one of the following:

If you have	Do this ...
An E2700, E5600, or EF560 storage array,	In SANtricity Storage Manager, select the Storage Array > Configuration > Automatic Load Balancing menu option to enable or disable the Automatic Load Balancing feature for an individual storage array.
An E2800 storage array,	In SANtricity System Manager, select Settings > System , scroll down to the Additional Settings section, click the Enable/Disable Automatic Load Balancing link, and select the Enable/Disable automatic load balancing checkbox to enable or disable the feature for an individual storage array.

Configuring virtualization and clustering

For load balancing, availability, and security concerns, virtualization and clustering are essential considerations for your storage configuration.

Related information

[*SANtricity Storage Manager 11.40 Installing and Configuring for VMware Express Guide*](#)

[*SANtricity System Manager 11.40 Installing and Configuring for VMware Express Guide*](#)

Virtualization considerations

For the purpose of storage, virtualization refers to the act of creating a virtual machine (VM) within a parent operating system. Virtualization isolates applications, and allows for virtual desktop deployments that can provide security not available on the physical operating system. In addition, virtualization can ensure high availability while reducing hardware costs across an enterprise. There are many virtualization technologies built onto operating systems, as well as operating systems whose main purpose is to provide virtualization.

Virtualization offers a wide range of capabilities to an organization:

- **Server consolidation:** Many servers can be replaced by one large physical server, so hardware is consolidated, and guest operating systems are converted to virtual machines. This consolidation provides the ability to run legacy software on new hardware.
- **Isolation:** A guest operating system can be fully isolated from the host running it. If the virtual machine is corrupted, the host system is not harmed.
- **Migration:** A process to move a running virtual machine to another physical machine. Live migration is an extended feature that allows this move without disconnection of the client or the application.
- **Disaster recovery:** Virtualized guest systems are less dependent on the hardware.

For virtualization deployments on NetApp E-Series products, storage volume layout and host mappings should be considered. Additionally, host multipathing and connection Pass-Thru might be required.

Storage volume layout

When planning your volume layout, the following general guidelines apply:

- The larger the deployment, the higher the disk count.
If volume groups or disk pools are not large enough, latency problems can cause a series of timeouts.
- As the volumes used by virtual machines increases within a volume group, the IO workload moves from mostly sequential to mostly random in pattern.
For example, one VMs workload will look sequential, but if you provide a series of VMs, the expanded workload will look random over time.

Volume Mapping & Pass Through

Volumes are typically mapped to the parent directory. Unless there are multiple RAID groups, NetApp recommends using one large disk for VMs. The large disk can later be divided into smaller segments for virtualization.

If copy services backup individual VMs, then volumes need to be mapped for each VM to the parent operating system. Some virtual environments allow storage to be managed by the virtual machine directly. This management requires you to define an additional host and host-type on the storage array to be configured.

Volumes mapped to this host are not visible to the parent operating system.

Multipathing and virtualization

Virtualization must account for multipathing software. In a typical virtualized environment, the parent operating system performs any failover scenarios required. If the VM is a pass thru, any pathing considerations need to be handled through failover within the VM.

Virtualization needs to account for multipathing software. In a typical virtualized environment, the parent os performs any failover scenarios required. If the VM is a pass thru, any pathing considerations need to be handled through failover within the VM.

When planning your installation, consider the following methods:

- **Single Root I/O Virtualization (SR-IOV)** is a specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or the guest operating system.

Host clustering support

Host clustering provides a way to load balance and make highly available applications. Generally, a cluster solution is one or more servers that work together and can be viewed as a single system. Cluster solutions improve performance and availability over a single computer, while being more cost-effective.

The following terms are common to a discussion of Host clustering:

Nodes

The underlying clients running the cluster application that make up the cluster. Traditionally, nodes pertained to physical servers, but some clustering packages allow virtual machines to also play the role of a node. In most cases, all nodes in a cluster use the same hardware and the same operating system.

Services

An entity shared by cluster nodes, Services are the high-level, tangible entities that depend on everything below them in the clustering hierarchy. Network shares and applications are examples of Services.

Services are monitored for accessibility and stability by the cluster application.

Resources

An entity shared by cluster notes, Resources are a lower-level entity than Services. Resources include entities like disks, and IP addresses.

Resources are exposed through services and monitored for accessibility and stability by the cluster application.

Cluster accessibility

Managing accessibility is critical for all cluster notes. The best methods for managing accessibility involve using a "heartbeat" for node-to-node communication, using "fencing" to control access to a cluster, and using a "quorum" to control the size of a cluster.

- **heartbeat:** All cluster nodes communicate with each other through a heartbeat. The most obvious communication method is through the network. If possible, the heartbeat should be on a separate

network. Clusters can also use serial cables or shared disks for communications. The heartbeat is so vital, that in some clusters a single dropped packet can result in a fenced node.

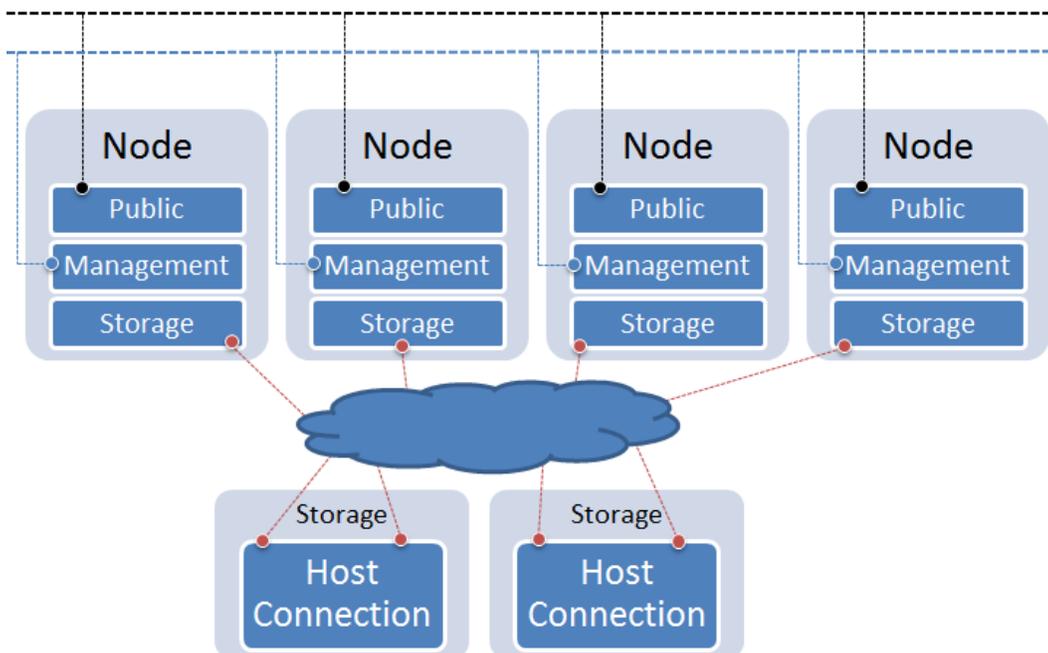
- **fencing:** The process nodes use to kick other nodes from a cluster. This process varies among cluster packages and can happen for a variety of reasons. Clusters usually have multiple types of fencing devices (ways to remove nodes from a cluster) including APC Power and SCSI Reservations.
- **quorum:** Some clusters adopt the idea of a quorum: a cluster is not be established until enough nodes have joined and agree that a cluster can be started. If enough nodes leave and there is no longer a quorum, the cluster can dissolve. Quorums can be established from the network or from shared disks (where a disk is called the quorum disk). Normally, quorum disks are more tolerant to node failures as network quorum requires a node majority ($N/2+1$).

Most clusters also have the concept of a failover domain. The failover domain determines which node will own the service at which time and can usually prioritize service migrations for load balancing.

Other clusters claim a "master node" in cases of failure. This method is not widely used because if the master node fails, the cluster can become 'split brain'. Split brain occurs when nodes are still claimed as active but do not have communications to other nodes who also claim to be active. The consequences can be devastating as similar services acting on the same resource can overwrite one another.

Cluster topology

Cluster connections consist of a public network, a private, cluster management network, and a storage network.



- **Public Network:** this network provides access to the outside world or LAN.
- **Private Network:** It is recommended to isolate a network specifically for cluster management. Some clustering software allow different management types (serial, network, etc).
- **Storage Network:** Traditional connections to storage. This can be a variety of protocols.

Cluster shared storage in SANtricity

Allowing multiple hosts to share the same storage is critical in many clusters.

About this task

Shared storage can be used in couple of ways by the cluster.

- **Shared Disk File System:** Some file systems are distributed aware. These file systems typically deploy a rigorous concurrency model to keep incoming data requests serialized.
- **General Parallel File System (GPFS):** A high-performance clustered file system that can be deployed in either shared-disk or shared-nothing distributed parallel modes. GPFS provides higher I/O performance by striping blocks of data from individual files over multiple disks, and reading and writing these blocks in parallel.
- **Quorum Disk:** Shared storage can provide a disk to the cluster designed to keep the cluster operational. If a node cannot access the quorum disk, then the node understands that it is no longer part of the cluster until access become available. Nodes communicate through the quorum disk to relay state information. This disk can be used in place of a heartbeat and can be the trigger for fencing behavior within the cluster.

To create shared storage in both SANtricity Storage Manager and SANtricity System Manager (if your storage array has an E2800 controller shelf), use the following general procedure, supplemented with online help topics:

Steps

1. Create all of the individual hosts that will share access to a set of volumes.
2. Do one of the following:
 - If you have an E2700, E5600, or EF560 controller shelf, create a host group.
 - If you have an E2800 controller shelf, create a host cluster.
3. Add all of the individual hosts to the host cluster or the host group.
4. Map all volumes into the host group or assign all volumes to the host cluster that you want to share.

When complete, all hosts can see the volume.

What are SCSI reservations?

SCSI reservations allow a node to lock volume access to other nodes. There are two types in use: SCSI-2 reservations and VAAI primitive Atomic Test and Set (ATS).

- SCSI-2 reservations provide two commands: `SCSI Reserve` and `SCSI Release`. A bus reset clears the LUN reservation. SCSI-2 reservations have been deprecated in recent standards, but are still available on various clusters.
- VAAI primitive atomic test and set: Hardware assisted locking, also called atomic test and set (ATS). Supports discrete virtual machine locking without use of SCSI reservations. This operation allows disk locking per sector, instead of per LUN as with SCSI reservations. ESXi uses ATS for VMFS datastores.

Deciding whether to use disk pools or volume groups

You can create volumes using either a disk pool or a volume group. The best selection depends primarily on your key storage requirements, such as expected I/O workload, performance requirements, and data protection requirements.

If you have a highly sequential workload and need maximum system bandwidth and the ability to tune storage settings, choose a volume group.

If you have a highly random workload and need faster drive rebuilds, simplified storage administration, and thin provisioning, choose a Dynamic Disk Pool (DDP).

Use case	Volume group	Dynamic Disk Pool
Workload - random	Good	Better
Workload - sequential	Better	Good
Drive rebuild times	Slower	Faster
Performance (optimal mode)	Good Best for large-block, sequential workloads	Good Best for small-block, random workloads
Performance (drive rebuild mode)	Degraded. Up to 40% drop in performance	Better
Multiple drive failure	Less data protection Slow rebuilds, greater risk of data loss	Greater data protection Faster, prioritized rebuilds
Adding drives	Slower Requires Dynamic Capacity Expansion operation	Faster Add to disk pool on the fly
Thin provisioning support	No	Yes
SSDs	Yes	Yes
Simplified administration	No Allocate global hot spares, configure RAID	Yes No hot spare or RAID settings to configure
Tunable performance	Yes	No

Creating a volume group

You use a volume group to create one or more volumes that are accessible to the host. A volume group is a container for volumes with shared characteristics such as RAID level and capacity.

About this task

With larger capacity drives and the ability to distribute volumes across controllers, creating more than one volume per volume group is a good way to make use of your storage capacity and to protect your data.

Follow these guidelines when you create a volume group.

- You need at least one unassigned drive.
- Limits exist as to how much drive capacity you can have in a single volume group. These limits vary according to your host type.
- To enable shelf/drawer loss protection, you must create a volume group that uses drives located in at least three shelves or drawers, unless you are using RAID 1, where two shelves/drawers is the minimum.

Review how your choice of RAID level affects the resulting capacity of the volume group.

- If you select RAID 1, you must add two drives at a time to make sure that a mirrored pair is selected. Mirroring and striping (known as RAID 10 or RAID 1+0) is achieved when four or more drives are selected.
- If you select RAID 5, you must add a minimum of three drives to create the volume group.
- If you select RAID 6, you must add a minimum of five drives to create the volume group.

Steps

1. Select **Storage > Pools & Volume Groups**.

2. Click **Create > Volume group**.

The Create Volume Group dialog box appears.

3. Type a name for the volume group.

4. Select the RAID level that best meets your requirements for data storage and protection.

The volume group candidate table appears and displays only the candidates that support the selected RAID level.

5. (Optional) If you have more than one type of drive in your storage array, select the drive type that you want to use.

The volume group candidate table appears and displays only the candidates that support the selected drive type and RAID level.

6. Select the volume group candidate that you want to use based on the following characteristics, and then click **Create**.

Characteristic	Use
Free Capacity	Shows the available capacity in GiB. Select a volume group candidate with the capacity for your application's storage needs.
Total Drives	Shows the number of drives available for this volume group. Select a volume group candidate with the number of drives that you want. The more drives that a volume group contains, the less likely it is that multiple drive failures will cause a critical drive failure in a volume group.

Characteristic	Use
Secure-Capable	<p>Indicates whether this volume group candidate is comprised entirely of secure-capable drives, which can be either Full Disk Encryption (FDE) drives or Federal Information Processing Standard (FIPS) drives.</p> <ul style="list-style-type: none"> You can protect your volume group with Drive Security, but all drives must be secure-capable to use this feature. If you want to create an FDE-only volume group, look for Yes - FDE in the Secure-Capable column. If you want to create a FIPS-only volume group, look for Yes - FIPS in the Secure-Capable column. You can create a volume group comprised of drives that might or might not be secure-capable or are a mix of security levels. If the drives in the volume group include drives that are not secure-capable, you cannot make the volume group secure.
Enable Security?	<p>Provides the option for enabling the Drive Security feature with secure-capable drives. If the volume group is secure-capable and you have set up a security key, you can enable Drive Security by selecting the check box.</p> <p>Note: The only way to remove Drive Security after it is enabled is to delete the volume group and erase the drives.</p>
DA Capable	<p>Indicates if Data Assurance (DA) is available for this group. Data Assurance (DA) checks for and corrects errors that might occur as data is communicated between a host and a storage array.</p> <p>If you want to use DA, select a volume group that is DA capable. This option is available only when the DA feature has been enabled.</p> <p>A volume group can contain drives that are DA-capable or not DA-capable, but all drives must be DA capable for you to use this feature.</p>
Shelf Loss Protection	<p>Shows if shelf loss protection is available.</p> <p>Shelf loss protection guarantees accessibility to the data on the volumes in a volume group if a total loss of communication to a shelf occurs.</p>
Drawer Loss Protection	<p>Shows if drawer loss protection is available, which is provided only if you are using a drive shelf that contains drawers.</p> <p>Drawer loss protection guarantees accessibility to the data on the volumes in a volume group if a total loss of communication occurs with a single drawer in a drive shelf.</p>

Creating a volume group using the AMW

Using SANtricity Storage Manager, you create a volume group, or a logical group of drives. You then designate a portion of the volume group as a volume to present to the host.

About this task

If you are using the Drive Security premium feature, make sure you understand how to implement it. For details, search for the Drive Security topic in the SANtricity Storage Manager Online Help.

Steps

1. Verify that hot spare coverage is adequate for the storage array.
 - a. From the **Array Management Window**, select **Hardware > Hot Spare Coverage**.
 - b. On the **Hot Spare Drive Options** dialog box, select **View/change current hot spare coverage** and select **OK**.
 - c. On the **Hot Spare Coverage** dialog box, view coverage to determine if you need to select more drives for hot spares.

Note: For help determining if coverage is adequate, select the hyperlink “*Tips on providing hot spare coverage*” on the Hot Spare Coverage dialog box.
 - d. If coverage is inadequate, select the **Assign** button and select hot spare drives on the **Assign Hot Spare** dialog box.
 - e. Select **Close**.
2. Select the **Storage & Copy Services** tab, right-click **Total Unconfigured Capacity**, and then select **Create Volume Group**.

Note: If there is more than one drive type, such as SAS and SSD drives, you cannot create a volume group from the high-level **Total Unconfigured Capacity** object. Instead, you must select a sub-object under that high-level object.
3. On the **Introduction** page of the wizard, select **Next**.
4. On the **Volume Group Name & Drive Selection** page of the wizard, perform the following steps:
 - a. Enter a name for the new volume group.
 - b. Select the **Automatic (Recommended)** radio button from the **Drive selection choices** list, and then select **Next**.
5. On the **RAID Level and Capacity** page, perform the following steps:
 - a. Select the desired RAID level for the new volume group from the drop-down list.

Note: For help determining the best RAID level, select the hyperlinks “*What RAID level is best for my application?*” and “*What is tray loss protection?*” on the RAID Level and Capacity page.
 - b. Select the desired volume group configuration from the list of available configurations and select **Finish**.
 - c. The **volume group** wizard automatically displays a prompt for you to create a volume in the newly created volume group. To create a volume immediately, select **Yes** to continue with the volume creation.

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. 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.

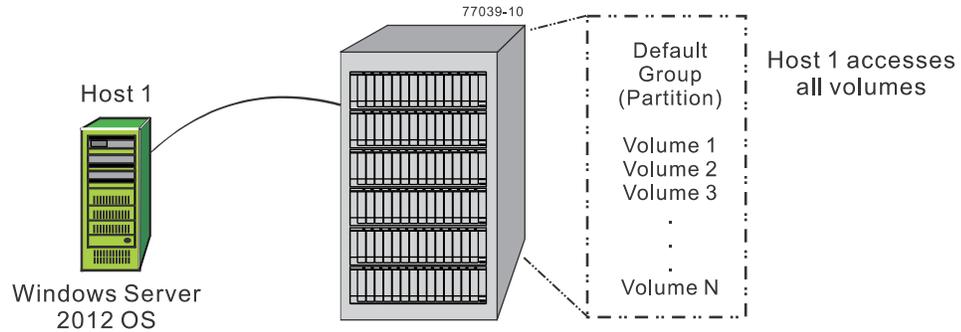
Note: If you have an E2800 controller shelf, storage partitioning is neither available nor needed on your system.

Note: If you must define a host group, you can define it through the Define Hosts Wizard described in the AMW online help.

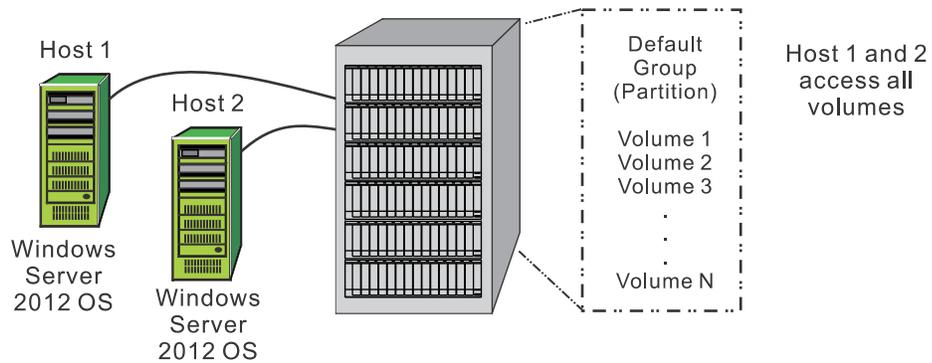
- You can think of a storage partition as a virtual storage array. That is, take the physical storage array and divide it up into multiple virtual storage arrays that you can then restrict to be accessible only by certain hosts.
- You do not create storage partitions in this step, but you must understand 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:



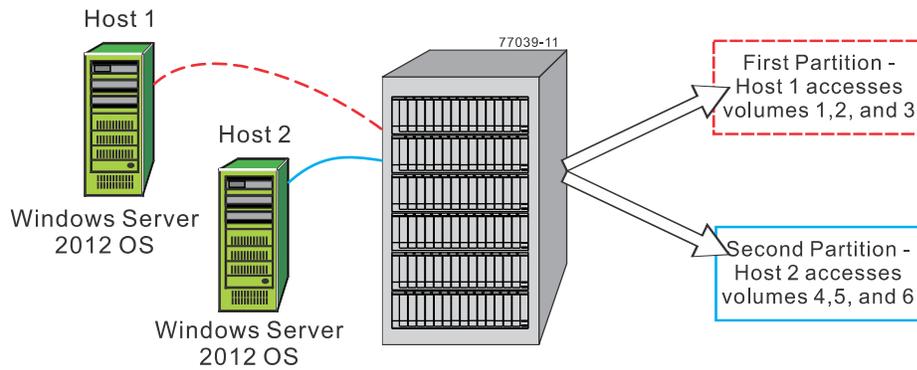
A single host accesses **all** volumes;
no additional storage partitions are needed.



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

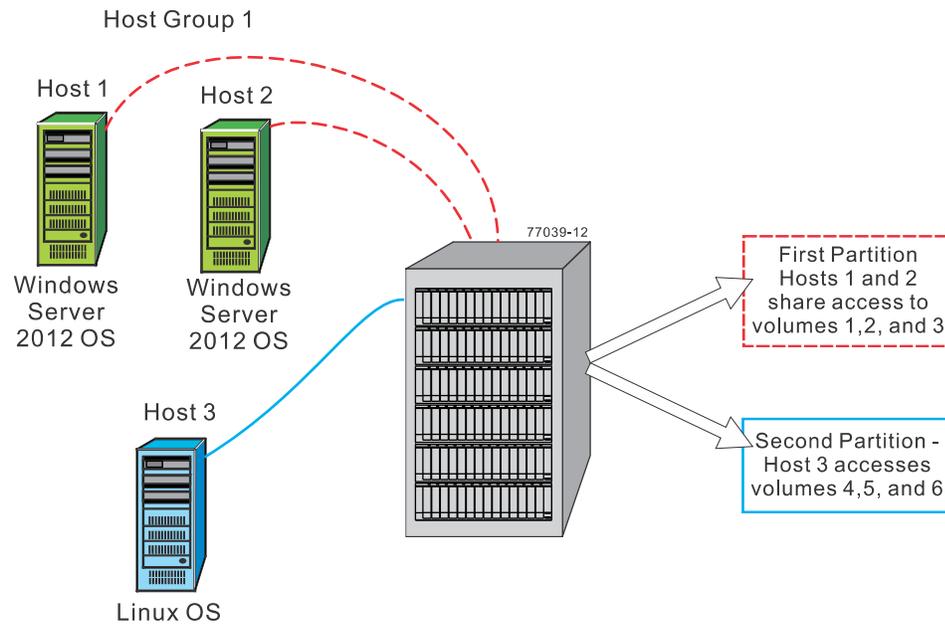
- You *do* need to create storage partitions if these conditions exist:
 - You want certain hosts to access only certain volumes.

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.

The following displays an example of additional storage partitions required (heterogeneous host):



- Host 1 and host 2 (Windows Server 2012 OS) share access to specific volumes through host group 1.
- Two heterogeneous hosts (Linux OS and Windows Server 2012 OS) exist.
- Host 3 (Linux) accesses specific volumes.
- Storage is divided into two logical storage partitions.
- A Default Group (partition) is not used.

Copyright information

Copyright © 1994–2017 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

Active IQ, AltaVault, Arch Design, ASUP, AutoSupport, Campaign Express, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Element, Fitness, Flash Accel, Flash Cache, Flash Pool, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, Fueled by SolidFire, GetSuccessful, Helix Design, LockVault, Manage ONTAP, MetroCluster, MultiStore, NetApp, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANscreen, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, SolidFire Helix, StorageGRID, SyncMirror, 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.

<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.

[*doccomments@netapp.com*](mailto: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