VMware express configuration

E-Series Systems

NetApp
November 09, 2022

Table of Contents

VMware express configuration

VMware express configuration overview

The VMware express method for installing your storage array and accessing SANtricity System Manager is appropriate for setting up a standalone VMware host to an E-Series storage system. It is designed to get the storage system up and running as quickly as possible with minimal decision points.

Procedure overview

The express method includes the following steps, which are also outlined in the VMware workflow.

1. Set up one of the following communication environments:
   - NVMe over Fibre Channel
   - Fibre Channel
   - iSCSI
   - SAS
2. Create logical volumes on the storage array.
3. Make the volumes available to the data host.

Find more information

- Online help — Describes how to use SANtricity System Manager to complete configuration and storage management tasks. It is available within the product.
- NetApp Knowledgebase (a database of articles) — Provides troubleshooting information, FAQs, and instructions for a wide range of NetApp products and technologies.
- NetApp Interoperability Matrix Tool — Enables you to search for configurations of NetApp products and components that meet the standards and requirements specified by NetApp.
- VMware Configuration Guide for E-Series SANtricity iSCSI Integration with ESXi 6.X — Provides technical details on iSCSI integration with VMware.
- VMware Configuration Maximums — Describes how to configure virtual and physical storage to stay within the allowed maximums that ESX/ESXi supports.
- Requirements and limitations of VMware NVMe storage.
- VMware vSphere Documentation — Provides ESXi vCenter Server documentation.

Assumptions

The VMware express method is based on the following assumptions:

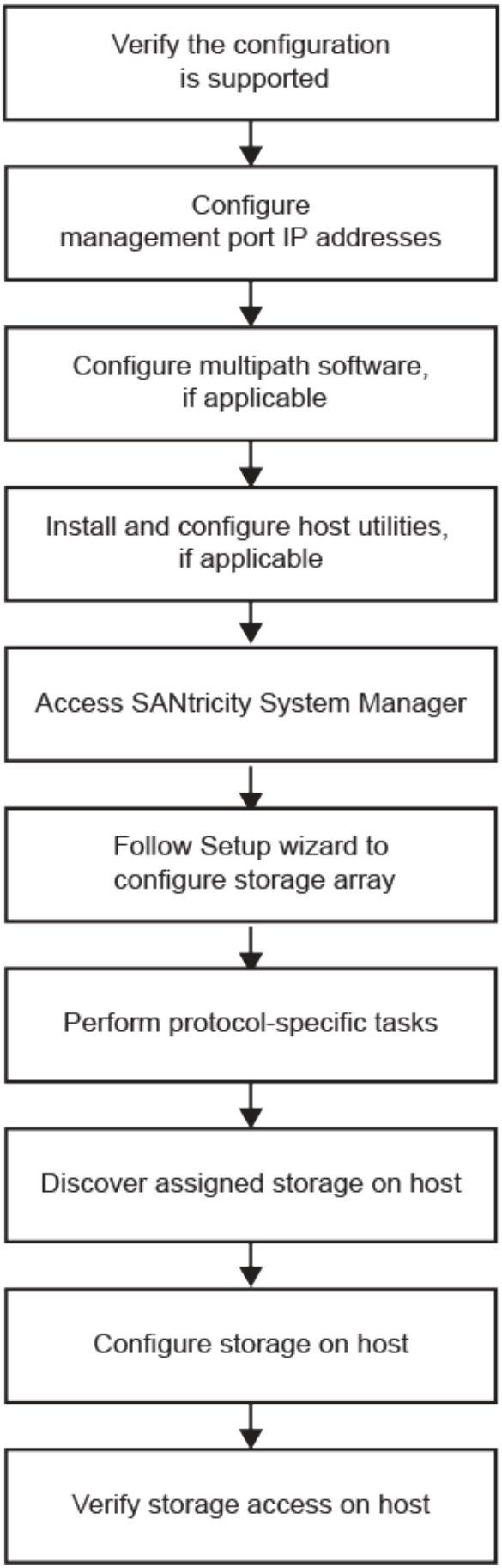
Component	Assumptions
Hardware	• You have used the Installation and Setup Instructions included with the controller shelves to install the hardware. • You have connected cables between the optional drive shelves and the controllers. • You have applied power to the storage system. • You have installed all other hardware (for example, management station, switches) and made the necessary connections.
Host	• You have made a connection between the storage system and the data host. • You have installed the host operating system. • You are not using VMware as a virtualized guest. • You are not configuring the data (I/O attached) host to boot from SAN.
Storage management station	• You are using a 1 Gbps or faster management network. • You are using a separate station for management rather than the data (I/O attached) host. • You are using out-of-band management, in which a storage management station sends commands to the storage system through the Ethernet connections to the controller. • You have attached the management station to the same subnet as the storage management ports.
IP addressing	• You have installed and configured a DHCP server. • You have **not** yet made an Ethernet connection between the management station and the storage system.
Storage provisioning	• You will not use shared volumes. • You will create pools rather than volume groups.
Protocol: FC	• You have made all host-side FC connections and activated switch zoning. • You are using NetApp-supported FC HBAs and switches. • You are using FC HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool.

Component	Assumptions
Protocol: NVMe over Fibre Channel	• You have made all host-side FC connections and activated switch zoning. • You are using NetApp-supported FC HBAs and switches. • You are using FC HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool.
Protocol: iSCSI	• You are using Ethernet switches capable of transporting iSCSI traffic. • You have configured the Ethernet switches according to the vendor's recommendation for iSCSI.
Protocol: SAS	• You are using NetApp-supported SAS HBAs. • You are using SAS HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool.

If these assumptions are not correct for your installation, or if you want more conceptual background information, see the following technical report: VMware Configuration Guide for E-Series SANtricity iSCSI Integration with ESXi 6.X

Understand the VMware workflow

This workflow guides you through the "express method" for configuring your storage array and SANtricity System Manager to make storage available to a VMware host.


Verify the configuration is supported
Configure management port IP addresses
Configure multipath software, if applicable
Install and configure host utilities, if applicable
Access SANtricity System Manager
Follow Setup wizard to configure storage array
Perform protocol-specific tasks
Discover assigned storage on host
Configure storage on host
Verify storage access on host

Verify the VMware configuration is supported

To ensure reliable operation, you create an implementation plan and then use the NetApp Interoperability Matrix Tool (IMT) to verify that the entire configuration is supported.

Steps

1. Go to the NetApp Interoperability Matrix Tool.
2. Click the **Solution Search** tile.
3. In the **Protocols › SAN Host** area, click the **Add** button next to **E-Series SAN Host**.
4. Click **View Refine Search Criteria**.

   The Refine Search Criteria section is displayed. In this section you may select the protocol that applies, as well as other criteria for the configuration such as Operating System, NetApp OS, and Host Multipath driver. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply. As necessary, make the updates for your operating system and protocol that are prescribed in the tool. Detailed information for your chosen configuration is accessible on the View Supported Configurations page by clicking the right page arrow.

5. As necessary, make the updates for your operating system and protocol as listed in the table.

Operating system updates	Protocol	Protocol-related updates
• You might need to install out-of-box drivers to ensure proper functionality and supportability. You can install HBA drivers using the ESXi shell or a remote SSH connection to the ESXi host. To access the host using either of those methods, you must enable the ESXi shell and SSH access. For more information about the ESXi shell, refer to the VMware Knowledge Base regarding using the ESXi shell in ESXi. For installation commands, refer to the instructions that accompany the HBA drivers. • Each HBA vendor has specific methods for updating boot code and firmware. Some of these methods could include the use of a vCenter plugin or the installation of CIM provider on the ESXi host. vCenter plugins can be used to obtain information about the vendor's specific HBA. Refer to the support section of the vendor's website to obtain the instructions and software necessary to update the HBA boot code or firmware. Refer to the *VMware Compatibility Guide* or the HBA vendor's website to obtain the correct boot code or firmware.	FC	Host bus adapter (HBA) driver, firmware, and bootcode
	iSCSI	Network interface card (NIC) driver, firmware and bootcode
	SAS	Host bus adapter (HBA) driver, firmware, and bootcode

Configure IP addresses using DHCP

To configure communications between the management station and the storage array, use Dynamic Host Configuration Protocol (DHCP) to provide IP addresses.

What you'll need

A DHCP server installed and configured on the same subnet as the storage management ports.

About this task

Each storage array has either one controller (simplex) or two controllers (duplex), and each controller has two storage management ports. Each management port will be assigned an IP address.

The following instructions refer to a storage array with two controllers (a duplex configuration).

Steps

1. If you have not already done so, connect an Ethernet cable to the management station and to management port 1 on each controller (A and B).

   The DHCP server assigns an IP address to port 1 of each controller.

   > Do not use management port 2 on either controller. Port 2 is reserved for use by NetApp technical personnel.

   > If you disconnect and reconnect the Ethernet cable, or if the storage array is power-cycled, DHCP assigns IP addresses again. This process occurs until static IP addresses are configured. It is recommended that you avoid disconnecting the cable or power-cycling the array.

   If the storage array cannot get DHCP-assigned IP addresses within 30 seconds, the following default IP addresses are set:

   - Controller A, port 1: 169.254.128.101
   - Controller B, port 1: 169.254.128.102
   - Subnet mask: 255.255.0.0

2. Locate the MAC address label on the back of each controller, and then provide your network administrator with the MAC address for port 1 of each controller.

   Your network administrator needs the MAC addresses to determine the IP address for each controller. You will need the IP addresses to connect to your storage system through your browser.

Configure the multipath software

To provide a redundant path to the storage array, you can configure multipath software.

Multipath software provides a redundant path to the storage array in case one of the physical paths is disrupted. The multipath software presents the operating system with a single virtual device that represents the active physical paths to the storage. The multipath software also manages the failover process that updates the virtual device. For VMware, NVMe/FC uses High Performance Plugin (HPP).

Applicable only for FC, iSCSI, and SAS protocols, VMware provides plug-ins, known as Storage Array Type Plug-ins (SATP), to handle the failover implementations of specific vendors' storage arrays.

The SATP you should use is **VMW_SATP_ALUA**.

For more information, see VMware SATPs.

Access SANtricity System Manager and use the Setup wizard

To configure your storage array, you can use the Setup wizard in SANtricity System Manager.

SANtricity System Manager is a web-based interface embedded on each controller. To access the user interface, you point a browser to the controller's IP address. A setup wizard helps you get started with system configuration.

What you'll need

- Out-of-band management.
- A management station for accessing SANtricity System Manager that includes one of the following browsers:

Browser	Minimum version
Google Chrome	79
Microsoft Internet Explorer	11
Microsoft Edge	79
Mozilla Firefox	70
Safari	12

About this task

If you are an iSCSI user, make sure you have closed the Setup wizard while configuring iSCSI.

The wizard automatically relaunches when you open System Manager or refresh your browser and *at least one* of the following conditions is met:

- No pools and volume groups are detected.
- No workloads are detected.
- No notifications are configured.

If the Setup wizard does not automatically appear, contact technical support.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

   `IPAddress` is the address for one of the storage array controllers.

   The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. For more information about the four local user roles, see the online help available in the SANtricity System Manager user interface.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

   The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Use the Setup wizard to perform the following tasks:
   - **Verify hardware (controllers and drives)** — Verify the number of controllers and drives in the storage array. Assign a name to the array.
   - **Verify hosts and operating systems** — Verify the host and operating system types that the storage array can access.
   - **Accept pools** — Accept the recommended pool configuration for the express installation method. A pool is a logical group of drives.
   - **Configure alerts** — Allow System Manager to receive automatic notifications when a problem occurs with the storage array.
   - **Enable AutoSupport** — Automatically monitor the health of your storage array and have dispatches sent to technical support.
4. If you have not already created a volume, create one by going to **Storage › Volumes › Create › Volume**.

> For EF300 and EF600, you must set the block size to 512 bytes to ensure compatibility with VMware. Refer to the SANtricity System Manager online help for more information on setting a volume to 512 bytes.

Perform FC-specific tasks

For the Fibre Channel protocol, you configure the switches and determine the host port identifiers.

> For EF300 and EF600, you must set the block size to 512 bytes to ensure compatibility with VMware. Refer to the SANtricity System Manager online help for more information on setting a volume to 512 bytes.

Step 1: Configure the FC switches—VMware

Configuring (zoning) the Fibre Channel (FC) switches enables the hosts to connect to the storage array and limits the number of paths. You zone the switches using the management interface for the switches.

What you'll need

- Administrator credentials for the switches.
- The WWPN of each host initiator port and of each controller target port connected to the switch. (Use your HBA utility for discovery.)

> A vendor's HBA utility can be used to upgrade and obtain specific information about the HBA. Refer to the support section of the vendor's website for instructions on how to obtain the HBA utility.

About this task

Each initiator port must be in a separate zone with all of its corresponding target ports. For details about zoning your switches, see the switch vendor's documentation.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.

2. Create a new zone that includes the first host initiator port and that also includes all of the target ports that connect to the same FC switch as the initiator.
3. Create additional zones for each FC host initiator port in the switch.
4. Save the zones, and then activate the new zoning configuration.

Step 2: Determine the host port WWPNs—FC

To configure FC zoning, you must determine the worldwide port name (WWPN) of each initiator port.

Steps

1. Connect to the ESXi host using SSH or the ESXi shell.
2. Run the following command:

```
esxcfg-scsidevs –a
```

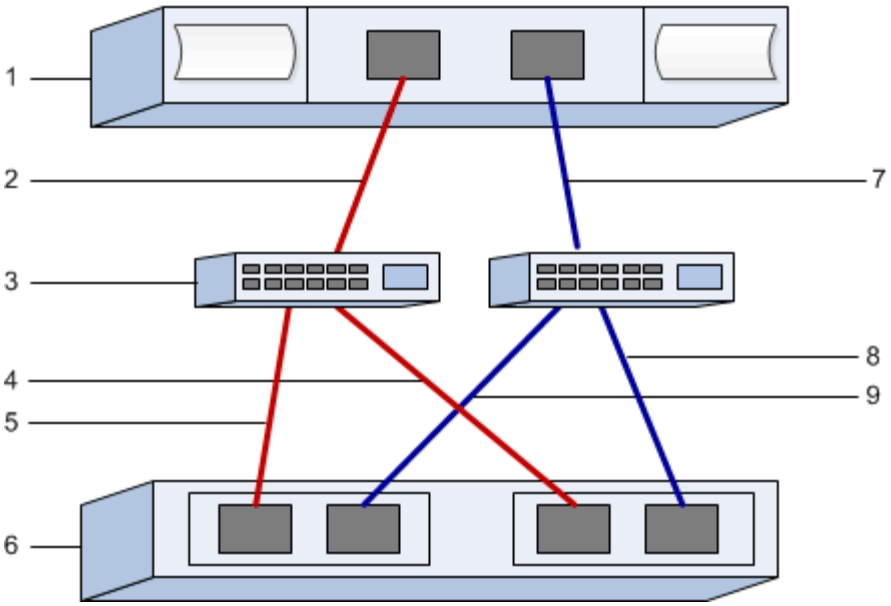
3. Record the initiator identifiers. The output will be similar to this example:

```
vmhba3 lpfc link-up  fc.20000090fa05e848:10000090fa05e848 (0000:03:00.0)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
vmhba4 lpfc link-up  fc.20000090fa05e849:10000090fa05e849 (0000:03:00.1)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
```

Step 3: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record FC storage configuration information. You need this information to perform provisioning tasks.

The illustration shows a host connected to an E-Series storage array in two zones. One zone is indicated by the blue line; the other zone is indicated by the red line. Each zone contains one initiator port and all target ports.



Host identifiers

Callout No.	Host (initiator) port connections	WWPN
1	Host	*not applicable*
2	Host port 0 to FC switch zone 0	
7	Host port 1 to FC switch zone 1	

Target identifiers

Callout No.	Array controller (target) port connections	WWPN
3	Switch	*not applicable*
6	Array controller (target)	*not applicable*
5	Controller A, port 1 to FC switch 1	
9	Controller A, port 2 to FC switch 2	
4	Controller B, port 1 to FC switch 1	
8	Controller B, port 2 to FC switch 2	

Mapping host

Mapping host name	

Host OS type	

Perform NVMe over FC-specific tasks

For the NVMe over Fibre Channel protocol, you configure the switches and determine the host port identifiers.

Step 1: Configure the NVMe/FC switches

Configuring (zoning) the NVMe over Fibre Channel (FC) switches enables the hosts to connect to the storage array and limits the number of paths. You zone the switches using the management interface for the switches.

What you'll need

- Administrator credentials for the switches.
- The WWPN of each host initiator port and of each controller target port connected to the switch. (Use your HBA utility for discovery.)

> A vendor's HBA utility can be used to upgrade and obtain specific information about the HBA. Refer to the support section of the vendor's website for instructions on how to obtain the HBA utility.

About this task

Each initiator port must be in a separate zone with all of its corresponding target ports. For details about zoning your switches, see the switch vendor's documentation.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first host initiator port and that also includes all of the target ports that connect to the same FC switch as the initiator.
3. Create additional zones for each FC host initiator port in the switch.
4. Save the zones, and then activate the new zoning configuration.

Step 2: Determine the host ports WWPNs—NVMe/FC VMware

To configure FC zoning, you must determine the worldwide port name (WWPN) of each initiator port.

Steps

1. Connect to the ESXi host using SSH or the ESXi shell.
2. Run the following command:

```
esxcfg-scsidevs –a
```

3. Record the initiator identifiers. The output will be similar to this example:

```
vmhba3 lpfc link-up  fc.20000090fa05e848:10000090fa05e848 (0000:03:00.0)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
vmhba4 lpfc link-up  fc.20000090fa05e849:10000090fa05e849 (0000:03:00.1)
Emulex Corporation Emulex LPe16000 16Gb PCIe Fibre Channel Adapter
```

Step 3: Enable HBA drivers

Support for NVMe must be enabled within Broadcom/Emulex and Marvell/Qlogic HBA drivers.

Steps

1. Execute one of the following commands from the ESXi shell:
   - **Broadcom/Emulex HBA Driver**

     ```
     esxcli system module parameters set -m lpfc -p
     "lpfc_enable_fc4_type=3"
     ```

   - **Marvell/Qlogic HBA Driver**

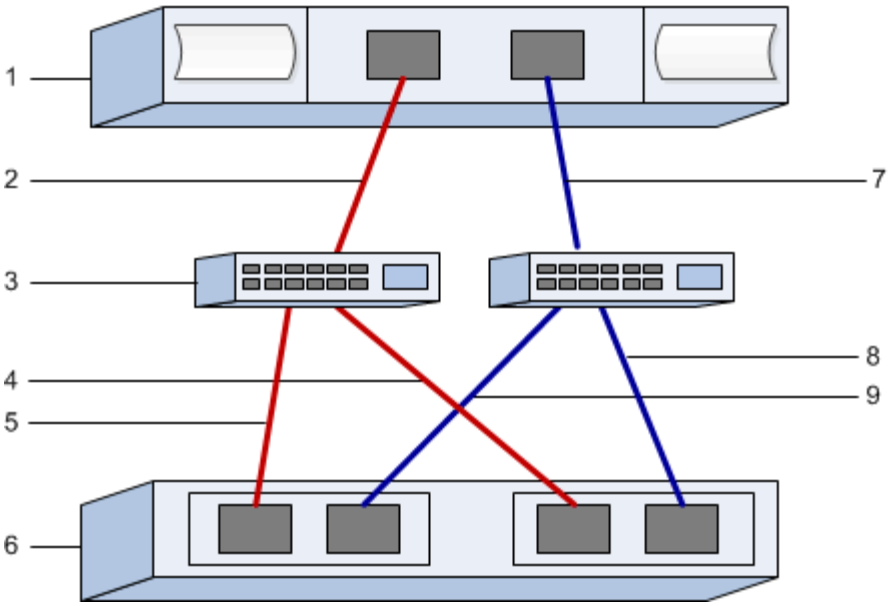
     ```
     esxcfg-module -s "ql2xnvmesupport=1" qlnativefc
     ```

2. Reboot the host.

Step 4: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record NVMe over Fibre Channel storage configuration information. You need this information to perform provisioning tasks.

The illustration shows a host connected to an E-Series storage array in two zones. One zone is indicated by the blue line; the other zone is indicated by the red line. Each zone contains one initiator port and all target ports.



Host identifiers

Callout No.	Host (initiator) port connections	WWPN
1	Host	*not applicable*
2	Host port 0 to FC switch zone 0	
7	Host port 1 to FC switch zone 1	

Target identifiers

Callout No.	Array controller (target) port connections	WWPN
3	Switch	*not applicable*
6	Array controller (target)	*not applicable*
5	Controller A, port 1 to FC switch 1	
9	Controller A, port 2 to FC switch 2	
4	Controller B, port 1 to FC switch 1	
8	Controller B, port 2 to FC switch 2	

Mapping host

Mapping host name	

Host OS type	

Perform iSCSI-specific tasks

For the iSCSI protocol, you configure the switches and configure networking on the array side and the host side. Then you verify the IP network connections.

Step 1: Configure the switches—iSCSI, VMware

You configure the switches according to the vendor's recommendations for iSCSI. These recommendations might include both configuration directives as well as code updates.

What you'll need

- Two separate networks for high availability. Make sure that you isolate your iSCSI traffic to separate network segments.
- Enabled send and receive hardware flow control **end to end**.
- Disabled priority flow control.
- If appropriate, enabled jumbo frames.

> Port channels/LACP is not supported on the controller's switch ports. Host-side LACP is not recommended; multipathing provides the same benefits or better.

Steps

Consult your switch vendor's documentation.

Step 2: Configure networking—iSCSI VMware

You can set up your iSCSI network in many ways, depending on your data storage requirements. Consult your network administrator for tips on selecting the best configuration for your environment.

What you'll need

- Enabled send and receive hardware flow control **end to end**.
- Disabled priority flow control.
- If appropriate, enabled jumbo frames.

  If you are using jumbo frames within the IP SAN for performance reasons, make sure to configure the array, switches, and hosts to use jumbo frames. Consult your operating system and switch documentation for information on how to enable jumbo frames on the hosts and on the switches. To enable jumbo frames on the array, complete the steps in Step 3.

About this task

While planning your iSCSI networking, remember that the VMware Configuration Maximums guide states that the maximum supported iSCSI storage paths is 8. You must consider this requirement to avoid configuring too many paths.

By default, the VMware iSCSI software initiator creates a single session per iSCSI target when you are not using iSCSI port binding.

VMware iSCSI port binding is a feature that forces all bound VMkernel ports to log into all target ports that are accessible on the configured network segments. It is meant to be used with arrays that present a single network address for the iSCSI target. NetApp recommends that iSCSI port binding not be used. For additional information, see the VMware Knowledge Base for the article regarding considerations for using software iSCSI port binding in ESX/ESXi. If the ESXi host is attached to another vendor's storage, NetApp recommends that you use separate iSCSI vmkernel ports to avoid any conflict with port binding.

For best practice, you should NOT use port binding on E-Series storage arrays.

To ensure a good multipathing configuration, use multiple network segments for the iSCSI network. Place at least one host-side port and at least one port from each array controller on one network segment, and an identical group of host-side and array-side ports on another network segment. Where possible, use multiple Ethernet switches to provide additional redundancy.

Steps

Consult your switch vendor's documentation.

Many network switches have to be configured above 9,000 bytes for IP overhead. Consult your switch documentation for more information.

Step 3: Configure array-side networking—iSCSI, VMware

You use the SANtricity System Manager GUI to configure iSCSI networking on the array side.

What you'll need

- The IP address or domain name for one of the storage array controllers.
- Password for the System Manager GUI, or Role-Based Access Control (RBAC) or LDAP and a directory service is configured for the appropriate security access to the storage array. See the SANtricity System Manager online help for more information about Access Management.

About this task

This task describes how to access the iSCSI port configuration from the Hardware page. You can also access the configuration from **System › Settings › Configure iSCSI ports**.

For additional information on how to set up the array-side networking on your VMware configuration, see the following technical report: VMware Configuration Guide for E-Series SANtricity iSCSI Integration with ESXi 6.x and 7.x.

Steps

1. From your browser, enter the following URL: `https://<DomainNameOrIPAddress>`

   `IPAddress` is the address for one of the storage array controllers.

   The first time SANtricity System Manager is opened on an array that has not been configured, the Set Administrator Password prompt appears. Role-based access management configures four local roles: admin, support, security, and monitor. The latter three roles have random passwords that cannot be guessed. After you set a password for the admin role, you can change all of the passwords using the admin credentials. See the SANtricity System Manager online help for more information on the four local user roles.

2. Enter the System Manager password for the admin role in the Set Administrator Password and Confirm Password fields, and then click **Set Password**.

   The Setup wizard launches if there are no pools, volumes groups, workloads, or notifications configured.

3. Close the Setup wizard.

   You will use the wizard later to complete additional setup tasks.

4. Select **Hardware**.
5. If the graphic shows the drives, click **Show back of shelf**.

   The graphic changes to show the controllers instead of the drives.

6. Click the controller with the iSCSI ports you want to configure.

   The controller's context menu appears.

7. Select **Configure iSCSI ports**.

   The Configure iSCSI Ports dialog box opens.

8. In the drop-down list, select the port you want to configure, and then click **Next**.
9. Select the configuration port settings, and then click **Next**.

   To see all port settings, click the **Show more port settings** link on the right of the dialog box.

Port Setting	Description
Configured ethernet port speed	Select the desired speed. The options that appear in the drop-down list depend on the maximum speed that your network can support (for example, 10 Gbps). The optional 25Gb iSCSI host interface cards available on the controllers do not auto-negotiate speeds. You must set the speed for each port to either 10 Gb or 25 Gb. All ports must be set to the same speed.
Enable IPv4 / Enable IPv6	Select one or both options to enable support for IPv4 and IPv6 networks.
TCP listening port (Available by clicking **Show more port settings**.)	If necessary, enter a new port number. The listening port is the TCP port number that the controller uses to listen for iSCSI logins from host iSCSI initiators. The default listening port is 3260. You must enter 3260 or a value between 49152 and 65535.

Port Setting	Description
MTU size (Available by clicking **Show more port settings**.)	If necessary, enter a new size in bytes for the Maximum Transmission Unit (MTU). The default Maximum Transmission Unit (MTU) size is 1500 bytes per frame. You must enter a value between 1500 and 9000.
Enable ICMP PING responses	Select this option to enable the Internet Control Message Protocol (ICMP). The operating systems of networked computers use this protocol to send messages. These ICMP messages determine whether a host is reachable and how long it takes to get packets to and from that host.

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

10. Configure the IPv4 and/or IPv6 settings, either automatically or manually. To see all port settings, click the **Show more settings** link on the right of the dialog box.

Port setting	Description
Automatically obtain configuration	Select this option to obtain the configuration automatically.
Manually specify static configuration	Select this option, and then enter a static address in the fields. For IPv4, include the network subnet mask and gateway. For IPv6, include the routable IP address and router IP address.

11. Click **Finish**.
12. Close System Manager.

Step 4: Configure host-side networking—iSCSI

Configuring iSCSI networking on the host side enables the VMware iSCSI initiator to establish a session with the array.

About this task

In this express method for configuring iSCSI networking on the host side, you allow the ESXi host to carry iSCSI traffic over four redundant paths to the storage.

After you complete this task, the host is configured with a single vSwitch containing both VMkernel ports and both VMNICs.

For additional information on configuring iSCSI networking for VMware, see the VMware vSphere Documentation for your version of vSphere.

Steps

1. Configure the switches that will be used to carry iSCSI storage traffic.
2. Enable send and receive hardware flow control **end to end**.
3. Disable priority flow control.
4. Complete the array side iSCSI configuration.
5. Use two NIC ports for iSCSI traffic.
6. Use either the vSphere client or vSphere web client to perform the host-side configuration.

   The interfaces vary in functionality and the exact workflow will vary.

Step 5: Verify IP network connections—iSCSI, VMware

You verify Internet Protocol (IP) network connections by using ping tests to ensure the host and array are able to communicate.

Steps

1. On the host, run one of the following commands, depending on whether jumbo frames are enabled:
   - If jumbo frames are not enabled, run this command:

     ```
     vmkping <iSCSI_target_IP_address\>
     ```

   - If jumbo frames are enabled, run the ping command with a payload size of 8,972 bytes. The IP and ICMP combined headers are 28 bytes, which when added to the payload, equals 9,000 bytes. The -s switch sets the `packet size` bit. The -d switch sets the DF (Don't Fragment) bit on the IPv4 packet. These options allow jumbo frames of 9,000 bytes to be successfully transmitted between the iSCSI initiator and the target.

     ```
     vmkping -s 8972 -d <iSCSI_target_IP_address\>
     ```

     In this example, the iSCSI target IP address is `192.0.2.8`.

     ```
     vmkping -s 8972 -d 192.0.2.8
     Pinging 192.0.2.8 with 8972 bytes of data:
     Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
     Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
     Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
     Reply from 192.0.2.8: bytes=8972 time=2ms TTL=64
     Ping statistics for 192.0.2.8:
       Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
     Approximate round trip times in milli-seconds:
       Minimum = 2ms, Maximum = 2ms, Average = 2ms
     ```

2. Issue a `vmkping` command from each host's initiator address (the IP address of the host Ethernet port

used for iSCSI) to each controller iSCSI port. Perform this action from each host server in the configuration, changing the IP addresses as necessary.

> If the command fails with the message `sendto() failed (Message too long)`, verify the MTU size (jumbo frame support) for the Ethernet interfaces on the host server, storage controller, and switch ports.

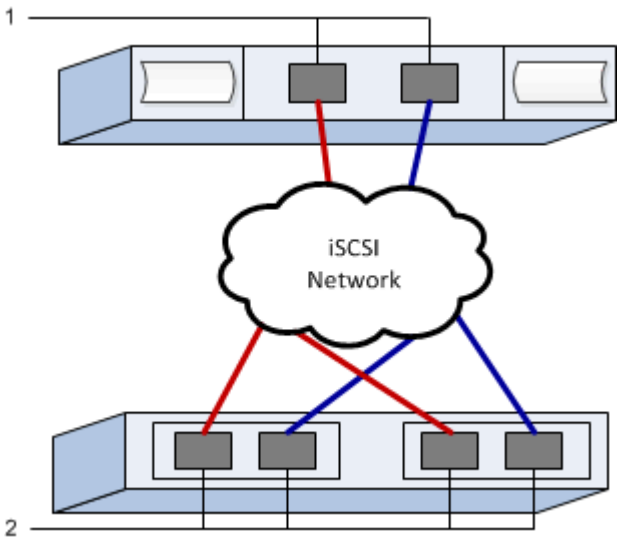
3. Return to the iSCSI Configuration procedure to finish target discovery.

Step 6: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record your protocol-specific storage configuration information. You need this information to perform provisioning tasks.

Recommended configuration

Recommended configurations consist of two initiator ports and four target ports with one or more VLANs.



Target IQN

Callout No.	Target port connection	IQN
2	Target port	

Mapping host name

Callout No.	Host information	Name and type
1	Mapping host name	
	Host OS type	

Perform SAS-specific tasks

For the SAS protocol, you determine host port addresses and make the recommended settings.

Step 1: Determine SAS host identifiers—VMware

Find the SAS addresses using the HBA utility, and then use the HBA BIOS to make the appropriate configuration settings.

About this task

Review the guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility.
- Host I/O ports might automatically register if the host context agent is installed.

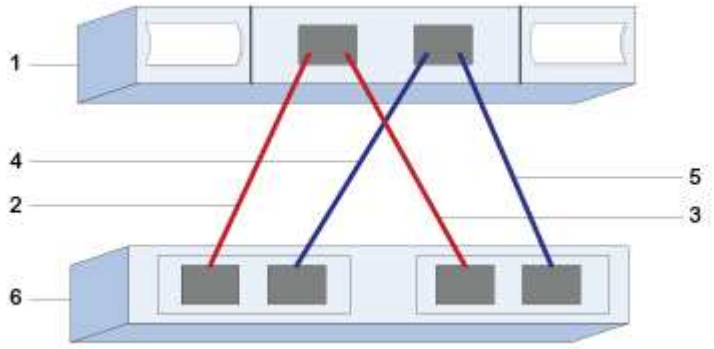
Steps

1. Download the HBA utility from your HBA vendor's web site.
2. Install the utility.
3. Use the HBA BIOS to select the appropriate settings for your configuration.

   For appropriate settings, see the Notes column of the NetApp Interoperability Matrix Tool for recommendations.

Step 2: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record your protocol-specific storage configuration information. You need this information to perform provisioning tasks.



Host identifiers

Callout No.	Host (initiator) port connections	SAS address
1	Host	*not applicable*

Callout No.	Host (initiator) port connections	SAS address
2	Host (initiator) port 1 connected to Controller A, port 1	
3	Host (initiator) port 1 connected to Controller B, port 1	
4	Host (initiator) port 2 connected to Controller A, port 1	
5	Host (initiator) port 2 connected to Controller B, port 1	

Target identifiers

Recommended configurations consist of two target ports.

Mapping host name

Mapping host name	
Host OS type	

Discover storage on the host

After assigning volumes to the host, you perform a rescan so that the host detects and configures the volumes for multipathing.

By default, an ESXi host automatically performs a rescan every five minutes. A volume might appear between the time you create it and assign it to a host, before you perform a manual rescan. Regardless, you can perform a manual rescan to ensure all volumes are configured properly.

Steps

1. Create one or more volumes and assign them to the ESXi host.
2. If using a vCenter Server, add the host to the server's inventory.
3. Use the vSphere Client or the vSphere Web Client to connect directly to the vCenter Server or to the ESXi host.
4. For instructions on how to perform a rescan of the storage on an ESXi host, search for the VMware Knowledge Base article on this topic.

Configure storage on the host

You can use the storage assigned to an ESXi host as either a Virtual Machine File System (VMFS) datastore or a raw device mapping (RDM). RDMs are not supported on the NVMe over Fibre Channel protocol.

All 6.*x* and 7 *x* versions of ESXi support VMFS versions 5 and 6.

Steps

1. Make sure the volumes mapped to the ESXi host have been discovered properly.
2. For instructions on creating VMFS datastores or using volumes as RDMs with either the vSphere Client or the vSphere Web Client, see the VMware Documentation web site.

Verify storage access on the host

Before using a volume, verify that the host can write data to the volume and read it back.

To do this, verify that the volume has been used as a Virtual Machine File System (VMFS) datastore or has been mapped directly to a VM for use as a raw device mapping (RDM).

Copyright information

Trademark information