Deploy software

E-Series Systems

NetApp
November 09, 2022

This PDF was generated from https://docs.netapp.com/us-en/e-series/config-linux/index.html on November 09, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Deploy software 1
Linux express configuration 1
VMware express configuration 144
Windows express configuration 165

Deploy software

Linux express configuration

Linux express configuration overview

The Linux express method for installing your storage array and accessing SANtricity System Manager is appropriate for setting up a standalone Linux 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 Linux express method includes the following steps.

1. Set up one of the following communication environments:
   - Fibre Channel (FC)
   - iSCSI
   - SAS
   - iSER over Infiniband
   - SRP over Infiniband
   - NVMe over Infiniband
   - NVMe over RoCE
   - NVMe over Fibre Channel
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.
- Linux Unified Host Utilities 7.1 Installation Guide — Describes how to use the Linux Unified Host Utilities 7.1.

Assumptions

The Linux 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. • If you are using NVMe over Infiniband, NVMe over RoCE, or NVMe over Fibre Channel, each EF300, EF600, EF570, or E5700 controller contains at least 32 GB of RAM.
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 Linux as a virtualized guest. • You are not configuring the data (I/O attached) host to boot from SAN. • You have installed any OS updates as listed under the NetApp Interoperability Matrix Tool.
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.

Component	Assumptions
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.
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.
Protocol: iSER over InfiniBand	• You are using an InfiniBand fabric. • You are using IB-iSER HBA driver and firmware versions as listed in the NetApp Interoperability Matrix Tool.
Protocol: SRP over InfiniBand	• You are using an InfiniBand fabric. • You are using IB-SRP driver and firmware versions as listed in the NetApp Interoperability Matrix Tool.
Protocol: NVMe over InfiniBand	• You have received the 100G or 200G host interface cards in an EF300, EF600, EF570, or E5700 storage system pre-configured with the NVMe over InfiniBand protocol or the controllers were ordered with standard IB ports and need to be converted to NVMe-oF ports. • You are using an InfiniBand fabric. • You are using NVMe/IB driver and firmware versions as listed in the NetApp Interoperability Matrix Tool.

Component	Assumptions
Protocol: NVMe over RoCE	• You have received the 100G or 200G host interface cards in an EF300, EF600, EF570, or E5700 storage system pre-configured with the NVMe over RoCE protocol or the controllers were ordered with standard IB ports and need to be converted to NVMe-oF ports. • You are using NVMe/RoCE driver and firmware versions as listed in the NetApp Interoperability Matrix Tool.
Protocol: NVMe over Fibre Channel	• You have received the 32G host interface cards in an EF300, EF600, EF570, or E5700 storage system pre-configured with the NVMe over Fibre Channel protocol or the controllers were ordered with standard FC ports and need to be converted to NVMe-oF ports. • You are using NVMe/FC driver and firmware versions as listed in the NetApp Interoperability Matrix Tool.

These express method instructions include examples for SUSE Linux Enterprise Server (SLES) and for Red Hat Enterprise Linux (RHEL).

Fibre Channel Express Setup

Verify the Linux 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 on 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.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. 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.

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.

Install and configure Linux Unified Host Utilities

The Linux Unified Host Utilities tools help you manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the NetApp Interoperability Matrix Tool to determine the appropriate version of Unified Host Utilities to install.

   The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from NetApp Support.

> Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

> If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **Disk space**: 5 GB
  - **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

Windows	Linux
Double-click the SMIA*.exe installation package to start the installation.	a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the `IATEMPDIR` variable. Example: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Run the `chmod +x SMIA*.bin` command to grant execute permission to the file. d. Run the `./SMIA*.bin` command to start the installer.

3. Use the installation wizard to install the software on the management station.

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

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.

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 more information, see the online help for SANtricity System Manager.

Configure the multipath software

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

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

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.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r
3.10.0-327.el7.x86_64
```

   You will use this information when you assign volumes to the host.

5. Enable the multipathd daemon on boot.

```
systemctl enable multipathd
```

6. Rebuild the `initramfs` image or the `initrd` image under /boot directory:

```
dracut --force --add multipath
```

7. Make sure that the newly created /boot/initrams-* image or /boot/initrd-* image is selected in the boot configuration file.

   For example, for grub it is `/boot/grub/menu.lst` and for grub2 it is `/boot/grub2/menu.cfg`.

8. Use the Create host manually procedure in the online help to check whether the hosts are defined. Verify that each host type setting is based on the kernel information gathered in step 4.

> Automatic Load Balancing is disabled for any volumes mapped to hosts running kernel 3.9 or earlier.

1. Reboot the host.

Set up the multipath.conf file

The multipath.conf file is the configuration file for the multipath daemon, multipathd.

The multipath.conf file overrides the built-in configuration table for multipathd.

For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

No changes to /etc/multipath.conf are required.

Configure the FC switches

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.)

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.

Determine host WWPNs and make the recommended settings

You install an FC HBA utility so you can view the worldwide port name (WWPN) of each host port.

Additionally, you can use the HBA utility to change any settings recommended in the Notes column of the NetApp Interoperability Matrix Tool for the supported configuration.

About this task

Review these guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility. You will need the correct version of HBA for your host operating system and CPU. Examples of FC HBA utilities include:
  - Emulex OneCommand Manager for Emulex HBAs
  - QLogic QConverge Console for QLogic HBAs
- Host I/O ports might automatically register if the host context agent is installed.

Steps

1. Download the appropriate utility from your HBA vendor's web site.

2. Install the utility.
3. Select the appropriate settings in the HBA utility.

   Appropriate settings for your configuration are listed in the Notes column of the NetApp Interoperability Matrix Tool.

Create partitions and filesystems

Because a new LUN has no partition or file system when the Linux host first discovers it, you must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the `ls` command in the /dev/mapper folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

   The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```
# sanlun lun show -p

                E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
                   Volume Name:
                Preferred Owner: Controller in Slot B
                  Current Owner: Controller in Slot B
                           Mode: RDAC (Active/Active)
                       UTM LUN: None
                           LUN: 116
                      LUN Size:
                       Product: E-Series
                   Host Device:
mpathr(360080e50004300ac000007575568851d)
               Multipath Policy: round-robin 0
             Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      controller                      controller
path      path       /dev/   host         target
state     type       node    adapter      port
--------- ---------- ------- ------------
----------------------------------------------
up        secondary  sdcx    host14       A1
up        secondary  sdat    host10       A2
up        secondary  sdbv    host13       B1
```

2. Create a new partition according to the method appropriate for your Linux OS release.

   Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. Create a file system on the partition.

   The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

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

What you'll need

An initialized volume that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

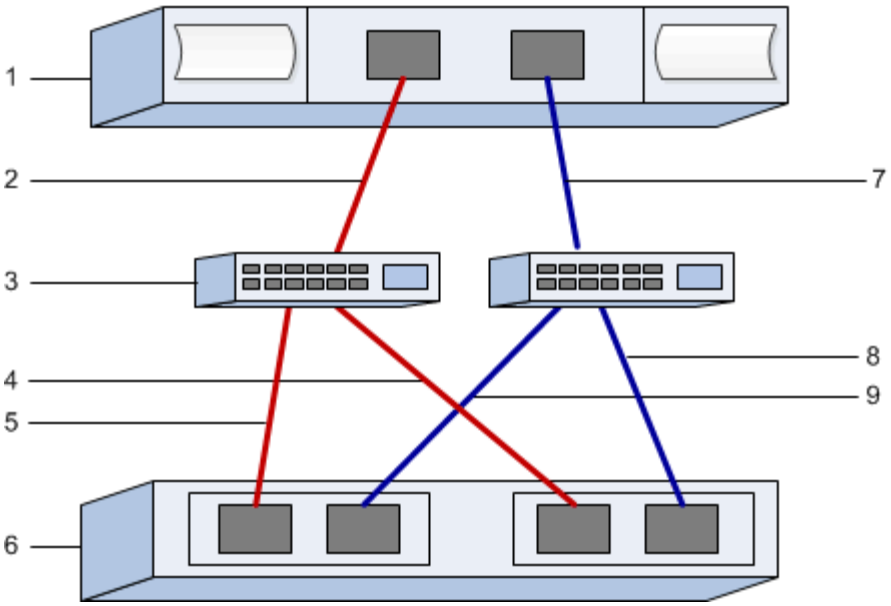
After you finish

Remove the file and folder that you copied.

Record your FC 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. Any single port has two paths to the storage (one to each controller).



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	

SAS Setup

Verify the Linux 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 on 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.

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.

Install and configure Linux Unified Host Utilities

The Linux Unified Host Utilities tools help you manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the NetApp Interoperability Matrix Tool to determine the appropriate version of Unified Host Utilities to install.

   The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from NetApp Support.

Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **Disk space**: 5 GB
  - **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

Windows	Linux
Double-click the SMIA*.exe installation package to start the installation.	a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the `IATEMPDIR` variable. Example: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Run the `chmod +x SMIA*.bin` command to grant execute permission to the file. d. Run the `./SMIA*.bin` command to start the installer.

3. Use the installation wizard to install the software on the management station.

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

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.

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 more information, see the online help for SANtricity System Manager.

Configure the multipath software

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

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

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.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

   ```
   # systemctl start multipathd
   ```

4. Save your kernel version by running the `uname -r` command.

   ```
   # uname -r
   3.10.0-327.el7.x86_64
   ```

   You will use this information when you assign volumes to the host.

5. Enable the `multipathd` daemon on boot.

```
systemctl enable multipathd
```

6. Rebuild the `initramfs` image or the `initrd` image under /boot directory:

```
dracut --force --add multipath
```

7. Make sure that the newly created /boot/initrams-* image or /boot/initrd-* image is selected in the boot configuration file.

   For example, for grub it is `/boot/grub/menu.lst` and for grub2 it is `/boot/grub2/menu.cfg`.

8. Use the Create host manually procedure in the online help to check whether the hosts are defined. Verify that each host type setting is based on the kernel information gathered in step 4.

> Automatic Load Balancing is disabled for any volumes mapped to hosts running kernel 3.9 or earlier.

1. Reboot the host.

Set up the multipath.conf file

The multipath.conf file is the configuration file for the multipath daemon, multipathd.

The multipath.conf file overrides the built-in configuration table for multipathd.

> For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

No changes to /etc/multipath.conf are required.

Determine SAS host identifiers - Linux

For the SAS protocol, you find the SAS addresses using the HBA utility, then use the HBA BIOS to make the appropriate configuration settings.

Before you begin this procedure, review these guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility. Depending on your host operating system and CPU, use either the LSI-sas2flash(6G) or sas3flash(12G) 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.

   See the Notes column of the NetApp Interoperability Matrix Tool for recommendations.

Create partitions and filesystems

A new LUN has no partition or file system when the Linux host first discovers it. You must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the `ls` command in the /dev/mapper folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

   The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```
# sanlun lun show -p

                E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
                   Volume Name:
                Preferred Owner: Controller in Slot B
                  Current Owner: Controller in Slot B
                           Mode: RDAC (Active/Active)
                       UTM LUN: None
                           LUN: 116
                      LUN Size:
                       Product: E-Series
                   Host Device:
mpathr(360080e50004300ac000007575568851d)
               Multipath Policy: round-robin 0
             Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      controller                      controller
path      path       /dev/   host         target
state     type       node    adapter      port
--------- ---------- ------- ------------
----------------------------------------------
up        secondary  sdcx    host14       A1
up        secondary  sdat    host10       A2
up        secondary  sdbv    host13       B1
```

2. Create a new partition according to the method appropriate for your Linux OS release.

   Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. Create a file system on the partition.

   The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

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

What you'll need

An initialized volume that is formatted with a file system.

Steps

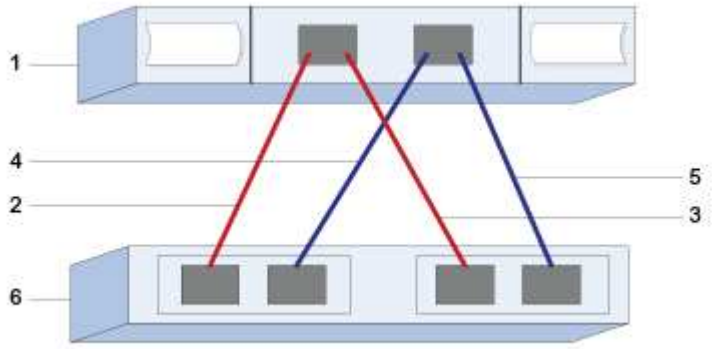
1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

Record your SAS configuration

You can generate and print a PDF of this page, and then use the following worksheet to record SAS 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

Mapping Host Name	
Host OS Type	

iSCSI Setup

Verify the Linux 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 on 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.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. 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.

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.

Install and configure Linux Unified Host Utilities

The Linux Unified Host Utilities tools help you manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the NetApp Interoperability Matrix Tool to determine the appropriate version of Unified Host Utilities to install.

   The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from NetApp Support.

> Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

> If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **Disk space**: 5 GB
  - **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

Windows	Linux
Double-click the SMIA*.exe installation package to start the installation.	a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the `IATEMPDIR` variable. Example: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Run the `chmod +x SMIA*.bin` command to grant execute permission to the file. d. Run the `./SMIA*.bin` command to start the installer.

3. Use the installation wizard to install the software on the management station.

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, you 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.

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 more information, see the online help for SANtricity System Manager.

Configure the multipath software

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

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

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.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r
3.10.0-327.el7.x86_64
```

   You will use this information when you assign volumes to the host.

5. Enable the `multipathd` daemon on boot.

```
systemctl enable multipathd
```

6. Rebuild the `initramfs` image or the `initrd` image under /boot directory:

```
dracut --force --add multipath
```

7. Use the Create host manually procedure in the online help to check whether the hosts are defined. Verify that each host type setting is based on the kernel information gathered in step 4.

> Automatic Load Balancing is disabled for any volumes mapped to hosts running kernel 3.9 or earlier.

1. Reboot the host.

Set up the multipath.conf file

The multipath.conf file is the configuration file for the multipath daemon, multipathd.

The multipath.conf file overrides the built-in configuration table for multipathd.

For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

No changes to /etc/multipath.conf are required.

Configure the switches

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

You must ensure the following:

- You have two separate networks for high availability. Make sure that you isolate your iSCSI traffic to separate network segments.
- You must enable flow control **end to end**.
- If appropriate, you have 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, and in some cases, better benefits.

Configure networking

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.

To configure an iSCSI network with basic redundancy, connect each host port and one port from each controller to separate switches, and partition each set of host ports and controller ports on separate network segments or VLANs.

You must enable send and receive hardware flow control **end to end**. You must disable priority flow control.

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 Configure array-side networking.

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

Configure array-side networking

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.
- A password for the System Manager GUI, or Role-Based Access Control (RBAC) or LDAP and a directory service 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 System Manager's Hardware page. You can also access the configuration from **System › Settings › Configure iSCSI ports**.

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. 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.
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.

Configure host-side networking

To configure host-side networking, you must perform several steps.

About this task

You configure iSCSI networking on the host side by setting the number of node sessions per physical path, turning on the appropriate iSCSI services, configuring the network for the iSCSI ports, creating iSCSI face bindings, and establishing the iSCSI sessions between initiators and targets.

In most cases, you can use the inbox software-initiator for iSCSI CNA/NIC. You do not need to download the latest driver, firmware, and BIOS. Refer to the NetApp Interoperability Matrix Tool to determine code requirements.

Steps

1. Check the `node.session.nr_sessions` variable in the /etc/iscsi/iscsid.conf file to see the default number of sessions per physical path. If necessary, change the default number of sessions to one session.

```
node.session.nr_sessions = 1
```

2. Change the `node.session.timeo.replacement_timeout` variable in the /etc/iscsi/iscsid.conf file to `20`, from a default value of `120`.

```
node.session.timeo.replacement_timeout=20
```

3. Make sure `iscsid` and `(open-)iscsi` services are on and enabled for boot.

Red Hat Enterprise Linux 7, 8, and 9 (RHEL 7, RHEL 8, and RHEL9)

```
# systemctl start iscsi
# systemctl start iscsid
# systemctl enable iscsi
# systemctl enable iscsid
```

SUSE Linux Enterprise Server 12 and 15 (SLES 12 and SLES 15)

```
# systemctl start iscsid.service
# systemctl enable iscsid.service
```

Optionally, you set `node.startup = automatic` in /etc/iscsi/iscsid.conf before running any `iscsiadm` commands to have sessions persist after reboot.

4. Get the host IQN initiator name, which will be used to configure the host to an array.

```
# cat /etc/iscsi/initiatorname.iscsi
```

5. Configure the network for iSCSI ports:

> In addition to the public network port, iSCSI initiators should use two or more NICs on separate private segments or vLANs.

   a. Determine the iSCSI port names using the `ifconfig -a` command.
   b. Set the IP address for the iSCSI initiator ports. The initiator ports should be present on the same subnet as the iSCSI target ports.

Red Hat Enterprise Linux 7, 8, and 9 (RHEL 7, RHEL 8, and RHEL9)

```
# vim /etc/sysconfig/network-scripts/ifcfg-<NIC port>
```

SUSE Linux Enterprise Server 12 and 15 (SLES 12 and SLES 15)

```
# vim /etc/sysconfig/network/ifcfg-<NIC port>
```

Edit:

```
BOOTPROTO=none
ONBOOT=yes
NM_CONTROLLED=no
```

Add:

```
IPADDR=192.168.xxx.xxx
NETMASK=255.255.255.0
```

> Be sure to set the address for both iSCSI initiator ports.

c. Restart network services.

```
# systemctl restart network
```

d. Make sure the Linux server can ping *all* of the iSCSI target ports.

6. Establish the iSCSI sessions between initiators and targets (four total).

a. When using ifaces, configure the iSCSI interfaces by creating two iSCSI iface bindings.

```
# iscsiadm -m iface -I iface0 -o new
# iscsiadm -m iface -I iface0 -o update -n iface.net_ifacename -v
<NIC port1>
```

```
# iscsiadm -m iface -I iface1 -o new
# iscsiadm -m iface -I iface1 -o update -n iface.net_ifacename -v
<NIC port2>
```

To list the interfaces, use `iscsiadm -m iface`.

b. Discover iSCSI targets. Save the IQN (it will be the same with each discovery) in the worksheet for the next step.

```
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260 -I iface0
-P 1
```

or

```
# iscsiadm -m discovery -t sendtargets -p 192.168.0.1:3260
```

The IQN looks like the following:

```
iqn.1992-01.com.netapp:2365.60080e50001bf1600000000531d7be3
```

c. Create the connection between the iSCSI initiators and iSCSI targets.

```
# iscsiadm -m node -T iqn.1992-
01.com.netapp:2365.60080e50001bf1600000000531d7be3
-p 192.168.0.1:3260 -I iface0 -l
```

or

```
# iscsiadm -m node -L all
```

d. List the iSCSI sessions established on the host.

```
# iscsiadm -m session
```

Verify IP network connections

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:

     ```
     ping -I <hostIP\> <targetIP\>
     ```

   - 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 debug option. These options allow jumbo frames of 9,000 bytes to be successfully transmitted between the iSCSI initiator and the target.

     ```
     ping -I <hostIP\> -s 8972 -d <targetIP\>
     ```

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

     ```
     #ping -I 192.0.2.100 -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 `ping` 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 (for example, returns `Packet needs to be fragmented but DF set`), verify the MTU size (jumbo frame support) for the Ethernet interfaces on the host server, storage controller, and switch ports.

Create partitions and filesystems

Because a new LUN has no partition or file system when the Linux host first discovers it, you must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the `ls` command in the /dev/mapper folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

   The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```
# sanlun lun show -p

                E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
                   Volume Name:
                Preferred Owner: Controller in Slot B
                  Current Owner: Controller in Slot B
                           Mode: RDAC (Active/Active)
                       UTM LUN: None
                           LUN: 116
                      LUN Size:
                       Product: E-Series
                   Host Device:
mpathr(360080e50004300ac000007575568851d)
               Multipath Policy: round-robin 0
            Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      controller                      controller
path      path       /dev/   host         target
state     type       node    adapter      port
--------- ---------- ------- ------------
----------------------------------------------
up        secondary  sdcx    host14       A1
up        secondary  sdat    host10       A2
up        secondary  sdbv    host13       B1
```

2. Create a new partition according to the method appropriate for your Linux OS release.

   Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. Create a file system on the partition.

   The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

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

What you'll need

An initialized volume that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

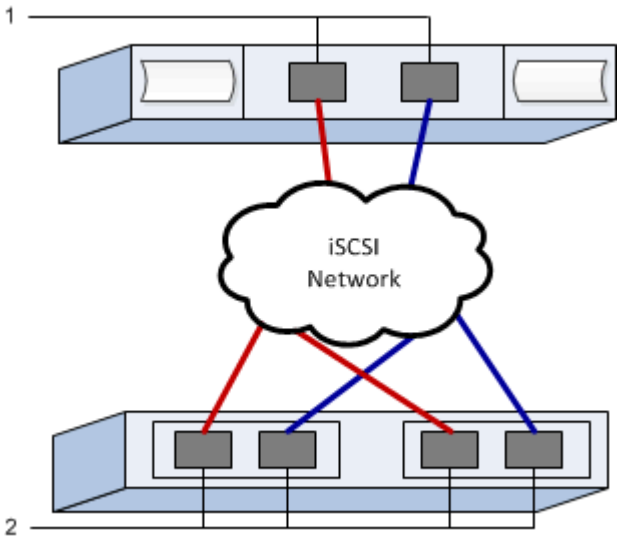
Remove the file and folder that you copied.

Record your iSCSI configuration

You can generate and print a PDF of this page, and then use the following worksheet to record iSCSI 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	

iSER over InfiniBand Setup

Verify the Linux 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 on 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.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. 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.

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.

Determine host port GUIDs and make the recommended settings

The infiniband-diags package includes commands to display the globally unique ID (GUID) of each InfiniBand (IB) port. Most Linux distributions with OFED/RDMA supported through the included packages also have the InfiniBand-diags package, which includes commands to display information about the HCA.

Steps

1. Install the InfiniBand-diags package using the operating system's package management commands.
2. Run the `ibstat` command to display the port information.
3. Record the initiator's GUIDs on the iSER over InfiniBand worksheet.
4. Select the appropriate settings in the HBA utility.

   Appropriate settings for your configuration are listed in the Notes column of the NetApp Interoperability Matrix Tool.

Configure subnet manager

A subnet manager must be running in your environment on your switch or on your hosts. If you are running it host-side, use the following procedure to set it up.

> Before configuring the subnet manager, you must install the infiniband-diags package to obtain the globally unique ID (GUID) through the `ibstat -p` command. See Determine host port GUIDs and make the recommended settings for information on how to install the infiniband-diags package.

Steps

1. Install the `opensm` package on any hosts that will be running the subnet manager.
2. Use the `ibstat -p` command to find `GUID0` and `GUID1` of the HBA ports. For example:

```
# ibstat -p
0x248a070300a80a80
0x248a070300a80a81
```

3. Create a subnet manager script that runs once as part of the boot process.

```
# vim /usr/sbin/subnet-manager.sh
```

4. Add the following lines. Substitute the values you found in step 2 for `GUID0` and `GUID1`. For `P0` and `P1`, use the subnet manager priorities, with 1 being the lowest and 15 the highest.

```
#!/bin/bash

opensm -B -g <GUID0> -p <P0> -f /var/log/opensm-ib0.log
opensm -B -g <GUID1> -p <P1> -f /var/log/opensm-ib1.log
```

   An example of the command with value substitutions:

```
#!/bin/bash

opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

5. Create a systemd service unit file named `subnet-manager.service`.

```
# vim /etc/systemd/system/subnet-manager.service
```

6. Add the following lines.

```
[Unit]
Description=systemd service unit file for subnet manager

[Service]
Type=forking
ExecStart=/bin/bash /usr/sbin/subnet-manager.sh

[Install]
WantedBy=multi-user.target
```

7. Notify systemd of the new service.

```
# systemctl daemon-reload
```

8. Enable and start the `subnet-manager` service.

```
# systemctl enable subnet-manager.service
# systemctl start subnet-manager.service
```

Install and configure Linux Unified Host Utilities

The Linux Unified Host Utilities tools help you manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the NetApp Interoperability Matrix Tool to determine the appropriate version of Unified Host Utilities to install.

   The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from NetApp Support.

> Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **Disk space**: 5 GB
  - **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

Windows	Linux
Double-click the SMIA*.exe installation package to start the installation.	a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the `IATEMPDIR` variable. Example: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Run the `chmod +x SMIA*.bin` command to grant execute permission to the file. d. Run the `./SMIA*.bin` command to start the installer.

3. Use the installation wizard to install the software on the management station.

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

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.

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 more information, see the online help for SANtricity System Manager.

Configure the multipath software

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

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

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.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r
3.10.0-327.el7.x86_64
```

You will use this information when you assign volumes to the host.

5. Enable the multipathd daemon on boot.

```
systemctl enable multipathd
```

6. Rebuild the `initramfs` image or the `initrd` image under /boot directory:

```
dracut --force --add multipath
```

7. Make sure that the newly created /boot/initrams-* image or /boot/initrd-* image is selected in the boot configuration file.

   For example, for grub it is `/boot/grub/menu.lst` and for grub2 it is `/boot/grub2/menu.cfg`.

8. Use the Create host manually procedure in the online help to check whether the hosts are defined. Verify that each host type setting is based on the kernel information gathered in step 4.

> Automatic Load Balancing is disabled for any volumes mapped to hosts running kernel 3.9 or earlier.

1. Reboot the host.

Set up the multipath.conf file

The multipath.conf file is the configuration file for the multipath daemon, multipathd.

The multipath.conf file overrides the built-in configuration table for multipathd.

> For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

No changes to /etc/multipath.conf are required.

Configure network connections

If your configuration uses the iSER over InfiniBand protocol, perform the steps in this section to configure network connections.

Steps

1. From System Manager, go to **Settings › System › Configure iSER over Infiniband Ports**. Refer to the System Manager online help for further instructions.

   Put the array iSCSI addresses on the same subnet as the host port(s) you will use to create iSCSI sessions. For addresses, see your iSER worksheet.

2. Record the IQN.

   This information might be necessary when you create iSER sessions from operating systems that do not

support send targets discovery. Enter this information in the iSER worksheet.

Configure networking for storage attached hosts

If your configuration uses the iSER over InfiniBand protocol, perform the steps in this section.

The InfiniBand OFED driver stack supports running both iSER and SRP simultaneously on the same ports, so no additional hardware is required.

What you'll need

A NetApp recommended OFED installed on the system. For more information, see the NetApp Interoperability Matrix Tool.

Steps

1. Enable and start iSCSI services on the host(s):

   Red Hat Enterprise Linux 7, 8, and 9 (RHEL 7, RHEL 8, and RHEL 9)

   ```
   # systemctl start iscsi
   # systemctl start iscsid
   # systemctl enable iscsi
   # systemctl enable iscsid
   ```

   SUSE Linux Enterprise Server 12 and 15 (SLES 12 and SLES 15)

   ```
   # systemctl start iscsid.service
   # systemctl enable iscsid.service
   ```

2. Configure InfiniBand card network interfaces:
   a. Identify the InfiniBand ports that will be used. Document the HW Address (MAC address) of each port.
   b. Configure persistent names for the InfiniBand network interface devices.
   c. Configure the IP address and network information for the InfiniBand interfaces identified.

      The specific interface configuration required might vary depending on the operating system used. Consult your vendor's operating system documentation for specific information on implementation.

   d. Start the IB network interfaces by restarting the networking service or by manually restarting each interface. For example:

      ```
      systemctl restart network
      ```

   e. Verify connectivity to the target ports. From the host, ping the IP addresses you configured when you configured network connections.
3. Restart services to load the iSER module.

4. Edit the iSCSI settings in /etc/iscsi/iscsid.conf.

```
node.startup = automatic
replacement_timeout = 20
```

5. Create iSCSI session configurations:

   a. Create iface configuration files for each InfiniBand interface.

   The directory location for the iSCSI iface files is operating system dependent. This example is for using Red Hat Enterprise Linux:

```
iscsiadm -m iface -I iser > /var/lib/iscsi/ifaces/iface-ib0
iscsiadm -m iface -I iser > /var/lib/iscsi/ifaces/iface-ib1
```

   b. Edit each iface file to set the interface name and initiator IQN. Set the following parameters appropriately for each iface file:

Option	Value
iface.net_ifacename	The interface device name (ex. ib0).
iface.initiatorname	The host initiator IQN documented in the worksheet.

   c. Create iSCSI sessions to the target.

   The preferred method to create the sessions is to use the SendTargets discovery method. However, this method does not work on some operating system releases.

   Use **Method 2** for RHEL 6.x or SLES 11.3 or later.

   - **Method 1 - SendTargets discovery:** Use the SendTargets discovery mechanism to one of the target portal IP addresses. This will create sessions for each of the target portals.

```
iscsiadm -m discovery -t st -p 192.168.130.101 -I iser
```

   - **Method 2 - Manual creation:** For each target portal IP address, create a session using the appropriate host interface iface configuration. In this example, interface ib0 is on subnet A and interface ib1 is on subnet B. For these variables, substitute the appropriate value from the worksheet:
     - <Target IQN> = storage array Target IQN
     - <Target Port IP> = IP address configured on the specified target port

```
# Controller A Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port IP\>
-l -o new
# Controller B Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port IP\>
-l -o new
# Controller A Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port IP\>
-l -o new
# Controller B Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port IP\>
-l -o new
```

6. Log in to iSCSI sessions.

   For each session, run the iscsiadm command to log in to the session.

```
# Controller A Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port IP\>
-l
# Controller B Port 1
iscsiadm -m node --target <Target IQN> -I iface-ib0 -p <Target Port IP\>
-l
# Controller A Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port IP\>
-l
# Controller B Port 2
iscsiadm -m node --target <Target IQN> -I iface-ib1 -p <Target Port IP\>
-l
```

7. Verify the iSER/iSCSI sessions.
   a. Check the iscsi session status from the host:

```
iscsiadm -m session
```

   b. Check the iscsi session status from the array. From SANtricity System Manager, navigate to **Storage Array** > **iSER** > **View/End Sessions**.

When the OFED/RDMA service starts, the iSER kernel module(s) loads by default when the iSCSI services are running. To complete the iSER connection setup, the iSER module(s) should be loaded. Currently this requires a host reboot.

Create partitions and filesystems

Because a new LUN has no partition or file system when the Linux host first discovers it, you must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the `ls` command in the /dev/mapper folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

   The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```
# sanlun lun show -p

                E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
                   Volume Name:
                Preferred Owner: Controller in Slot B
                  Current Owner: Controller in Slot B
                           Mode: RDAC (Active/Active)
                       UTM LUN: None
                           LUN: 116
                      LUN Size:
                       Product: E-Series
                   Host Device:
mpathr(360080e50004300ac000007575568851d)
               Multipath Policy: round-robin 0
             Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      controller                      controller
path      path       /dev/   host         target
state     type       node    adapter      port
--------- ---------- ------- ------------
----------------------------------------------
up        secondary  sdcx    host14       A1
up        secondary  sdat    host10       A2
up        secondary  sdbv    host13       B1
```

2. Create a new partition according to the method appropriate for your Linux OS release.

   Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. Create a file system on the partition.

   The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

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

What you'll need

An initialized volume that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

Record your iSER over IB configuration

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

Host identifiers

The software initiator IQN is determined during the task, Configure networking for storage attached hosts.

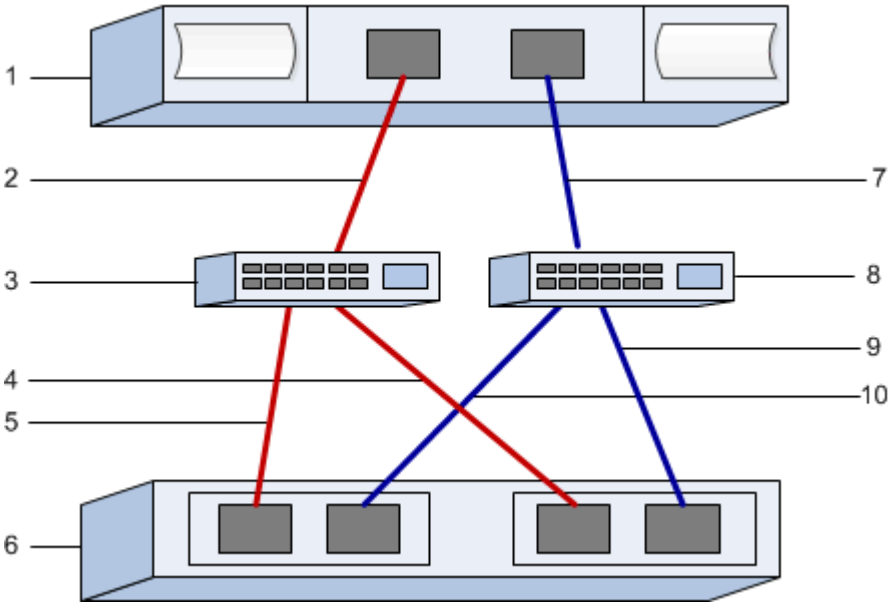
Locate and document the initiator IQN from each host. For software initiators, the IQN is typically found in the /etc/iscsi/initiatorname.iscsi file.

Callout No.	Host port connections	Software initiator IQN
1	Host (initiator) 1	
n/a		
n/a		
n/a		

Callout No.	Host port connections	Software initiator IQN
n/a		

Recommended configuration

Recommended configurations consist of two host (initiator) ports and four target ports.



Target IQN

Document the target IQN for the storage array. You will use this information in Configure networking for storage attached hosts.

Find the Storage Array IQN name using SANtricity: **Storage Array** > **iSER** > **Manage Settings**. This information might be necessary when you create iSER sessions from operating systems that do not support send targets discovery.

Callout No.	Array name	Target IQN
6	Array controller (target)	

Network configuration

Document the network configuration that will be used for the hosts and storage on the InfiniBand fabric. These instructions assume that two subnets will be used for full redundancy.

Your network administrator can provide the following information. You use this information in the topic, Configure networking for storage attached hosts.

Subnet A

Define the subnet to be used.

Network Address	Netmask

Document the IQNs to be used by the array ports and each host port.

Callout No.	Array controller (target) port connections	IQN
3	Switch	*not applicable*
5	Controller A, port 1	
4	Controller B, port 1	
2	Host 1, port 1	
	(Optional) Host 2, port 1	

Subnet B

Define the subnet to be used.

Network Address	Netmask

Document the IQNs to be used by the array ports and each host port.

Callout No.	Array controller (target) port connections	IQN
8	Switch	*not applicable*
10	Controller A, port 2	
9	Controller B, port 2	
7	Host 1, port 2	
	(Optional) Host 2, port 2	

Mapping host name

The mapping host name is created during the workflow.

Mapping host name	
Host OS type	

SRP over InfiniBand Setup

Verify the Linux 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 on 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.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. 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.

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.

Determine host port GUIDs and make the recommended settings

The infiniband-diags package includes commands to display the globally unique ID (GUID) of each InfiniBand (IB) port. Most Linux distributions with OFED/RDMA supported through the included packages also have the infiniband-diags package, which includes commands to display information about the HCA.

Steps

1. Install the `infiniband-diags` package using the operating system's package management commands.
2. Run the `ibstat` command to display the port information.
3. Record the initiator's GUIDs on the SRP worksheet.
4. Select the appropriate settings in the HBA utility.

   Appropriate settings for your configuration are listed in the Notes column of the NetApp Interoperability Matrix Tool.

Configure subnet manager

A subnet manager must be running in your environment on your switch or on your hosts. If you are running it host-side, use the following procedure to set it up.

Before configuring the subnet manager, you must install the infiniband-diags package to obtain the globally unique ID (GUID) through the `ibstat -p` command. See Determine host port GUIDs and make the recommended settings for information on how to install the infiniband-diags package.

Steps

1. Install the `opensm` package on any hosts that will be running the subnet manager.
2. Use the `ibstat -p` command to find `GUID0` and `GUID1` of the HBA ports. For example:

```
# ibstat -p
0x248a070300a80a80
0x248a070300a80a81
```

3. Create a subnet manager script that runs once as part of the boot process.

```
# vim /usr/sbin/subnet-manager.sh
```

4. Add the following lines. Substitute the values you found in step 2 for `GUID0` and `GUID1`. For `P0` and `P1`, use the subnet manager priorities, with 1 being the lowest and 15 the highest.

```
#!/bin/bash

opensm -B -g <GUID0> -p <P0> -f /var/log/opensm-ib0.log
opensm -B -g <GUID1> -p <P1> -f /var/log/opensm-ib1.log
```

An example of the command with value substitutions:

```
#!/bin/bash

opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

5. Create a systemd service unit file named `subnet-manager.service`.

```
# vim /etc/systemd/system/subnet-manager.service
```

6. Add the following lines.

```
[Unit]
Description=systemd service unit file for subnet manager

[Service]
Type=forking
ExecStart=/bin/bash /usr/sbin/subnet-manager.sh

[Install]
WantedBy=multi-user.target
```

7. Notify systemd of the new service.

```
# systemctl daemon-reload
```

8. Enable and start the `subnet-manager` service.

```
# systemctl enable subnet-manager.service
# systemctl start subnet-manager.service
```

Install and configure Linux Host Utilities

The Linux Unified Host Utilities package includes tools to manage NetApp storage, including failover policies and physical paths.

Steps

1. Use the NetApp Interoperability Matrix Tool to determine the appropriate version of Unified Host Utilities to install.

   The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from NetApp Support.

> Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

> If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine

- **Disk space**: 5 GB
- **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

Windows	Linux
Double-click the SMIA*.exe installation package to start the installation.	a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the `IATEMPDIR` variable. Example: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Run the `chmod +x SMIA*.bin` command to grant execute permission to the file. d. Run the `./SMIA*.bin` command to start the installer.

3. Use the installation wizard to install the software on the management station.

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

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

About this task

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.

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 more information, see the online help for SANtricity System Manager.

Configure the multipath software

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

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`.
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`.

If you have not already installed the operating system, use the media supplied by your operating system vendor.

About this task

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.

You use the device mapper multipath (DM-MP) tool for Linux installations. By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. If a multipath.conf file is not already created, run the `# touch /etc/multipath.conf` command.
2. Use the default multipath settings by leaving the multipath.conf file blank.
3. Start the multipath service.

```
# systemctl start multipathd
```

4. Save your kernel version by running the `uname -r` command.

```
# uname -r
3.10.0-327.el7.x86_64
```

   You will use this information when you assign volumes to the host.

5. Enable the `multipathd` daemon on boot.

```
systemctl enable multipathd
```

6. Rebuild the `initramfs` image or the `initrd` image under /boot directory:

```
dracut --force --add multipath
```

7. Make sure that the newly created /boot/initrams-* image or /boot/initrd-* image is selected in the boot configuration file.

   For example, for grub it is `/boot/grub/menu.lst` and for grub2 it is `/boot/grub2/menu.cfg`.

8. Use the Create host manually procedure in the online help to check whether the hosts are defined. Verify that each host type setting is based on the kernel information gathered in step 4.

> Automatic Load Balancing is disabled for any volumes mapped to hosts running kernel 3.9 or earlier.

1. Reboot the host.

Set up the multipath.conf file

The multipath.conf file is the configuration file for the multipath daemon, multipathd.

The multipath.conf file overrides the built-in configuration table for multipathd.

> For SANtricity operating system 8.30 and newer, NetApp recommends using the default settings as provided.

No changes to /etc/multipath.conf are required.

Configure network connections—SRP over Infiniband

If your configuration uses the SRP over Infiniband protocol, follow the steps in this section.

What you'll need

To connect the Linux host to the storage array, you must enable the InfiniBand driver stack with the appropriate options. Specific settings might vary between Linux distributions. Check the NetApp Interoperability Matrix Tool for specific instructions and additional recommended settings specific to your solution.

Steps

1. Install the OFED/RDMA driver stack for your OS.

   SLES

   ```
   zypper install rdma-core
   ```

   RHEL

   ```
   yum install rdma-core
   ```

2. Configure OFED/RDMA to load the SRP module.

   SLES

   ```
   zypper install srp_daemon
   ```

   RHEL

   ```
    yum install srp_daemon
   ```

3. In the OFED/RDMA configuration file, set `SRP_LOAD=yes` and `SRP_DAEMON_ENABLE=yes`.

   The RDMA configuration file is located at the following location:

   ```
   /etc/rdma/rdma.conf
   ```

4. Enable and start the OFED/RDMA service.

   RHEL 7.x and SLES 12.x or greater

   - To enable the InfiniBand modules to load on boot:

     ```
     systemctl enable rdma
     ```

   - To load the InfiniBand modules immediately:

     ```
     systemctl start rdma
     ```

5. Enable the SRP daemon.

   RHEL 7.x and SLES 12 or greater

   - To enable the SRP daemon to start on boot:

     ```
     systemctl enable srp_daemon
     ```

   - To start the SRP daemon immediately:

     ```
     systemctl start srp_daemon
     ```

6. If you need to modify the SRP configuration, enter the following command to create `/etc/modprobe.d/ib_srp.conf`.

```
options ib_srp cmd_sg_entries=255 allow_ext_sg=y
indirect_sg_entries=2048
```

a. Under the `/etc/srp_daemon.conf`, add the following line.

```
a    max_sect=4096
```

Create partitions and filesystems

Because a new LUN has no partition or file system when the Linux host first discovers it, you must format the LUN before it can be used. Optionally, you can create a file system on the LUN.

What you'll need

- A LUN that is discovered by the host.
- A list of available disks. (To see available disks, run the `ls` command in the /dev/mapper folder.)

About this task

You can initialize the disk as a basic disk with a GUID partition table (GPT) or Master boot record (MBR).

Format the LUN with a file system such as ext4. Some applications do not require this step.

Steps

1. Retrieve the SCSI ID of the mapped disk by issuing the `sanlun lun show -p` command.

   The SCSI ID is a 33-character string of hexadecimal digits, beginning with the number 3. If user-friendly names are enabled, Device Mapper reports disks as mpath instead of by a SCSI ID.

```
# sanlun lun show -p

                E-Series Array: ictm1619s01c01-
SRP(60080e50002908b40000000054efb9d2)
                   Volume Name:
                Preferred Owner: Controller in Slot B
                  Current Owner: Controller in Slot B
                           Mode: RDAC (Active/Active)
                       UTM LUN: None
                           LUN: 116
                      LUN Size:
                       Product: E-Series
                   Host Device:
mpathr(360080e50004300ac000007575568851d)
               Multipath Policy: round-robin 0
             Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      controller                      controller
path      path       /dev/   host         target
state     type       node    adapter      port
--------- ---------- ------- ------------
----------------------------------------------
up        secondary  sdcx    host14       A1
up        secondary  sdat    host10       A2
up        secondary  sdbv    host13       B1
```

2. Create a new partition according to the method appropriate for your Linux OS release.

   Typically, characters identifying the partition of a disk are appended to the SCSI ID (the number 1 or p3 for instance).

```
# parted -a optimal -s -- /dev/mapper/360080e5000321bb8000092b1535f887a
mklabel
gpt mkpart primary ext4 0% 100%
```

3. Create a file system on the partition.

   The method for creating a file system varies depending on the file system chosen.

```
# mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
```

4. Create a folder to mount the new partition.

```
# mkdir /mnt/ext4
```

5. Mount the partition.

```
# mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
```

Verify storage access on the host

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

What you'll need

An initialized volume that is formatted with a file system.

Steps

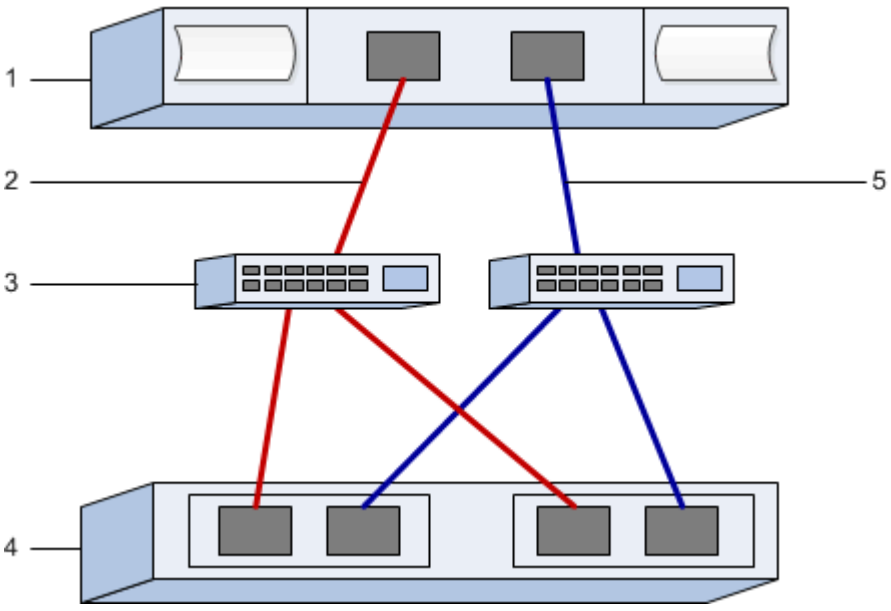
1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

Record your SRP over IB configuration

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



Host identifiers

The initiator GUIDs are determined in the task, Determine host port GUIDs and make the recommended settings.

Callout No.	Host (initiator) port connections	GUID
1	Host	*not applicable*
3	Switch	*not applicable*
4	Target (storage array)	*not applicable*
2	Host port 1 to IB switch 1 ("A" path)	
5	Host port 2 to IB switch 2 ("B" path)	

Recommended configuration

Recommended configurations consist of two initiator ports and four target ports.

Mapping host name

The mapping host name is created during the workflow.

Mapping host name	
Host OS type	

NVMe over InfiniBand Setup

Verify Linux support and review restrictions

As a first step, you should verify that your Linux configuration is supported and also review the controller, host, and recovery restrictions.

Verify the Linux 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 on 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.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. 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.

Review NVMe over InfiniBand restrictions

Before using NVMe over InfiniBand, see the NetApp Interoperability Matrix Tool to review the latest controller, host, and recovery restrictions.

Storage and disaster recovery restrictions

- Asynchronous and synchronous mirroring are not supported.
- Thin provisioning (the creation of thin volumes) is not supported.

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.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

> If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **Disk space**: 5 GB
  - **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

Windows	Linux
Double-click the SMIA*.exe installation package to start the installation.	a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the `IATEMPDIR` variable. Example: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Run the `chmod +x SMIA*.bin` command to grant execute permission to the file. d. Run the `./SMIA*.bin` command to start the installer.

3. Use the installation wizard to install the software on the management station.

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

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.

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 more information, see the online help for SANtricity System Manager.

Determine host port GUIDs and make the recommended settings

The infiniband-diags package includes commands to display the globally unique ID (GUID) of each InfiniBand (IB) port. Most Linux distributions with OFED/RDMA supported through the included packages also have the infiniband-diags package, which includes commands to display information about the HCA.

Steps

1. Install the `infiniband-diags` package using the operating system's package management commands.
2. Run the `ibstat` command to display the port information.
3. Record the initiator's GUIDs on the SRP worksheet.
4. Select the appropriate settings in the HBA utility.

   Appropriate settings for your configuration are listed in the Notes column of the NetApp Interoperability

Matrix Tool.

Configure subnet manager

A subnet manager must be running in your environment on your switch or on your hosts. If you are running it host-side, use the following procedure to set it up.

> Before configuring the subnet manager, you must install the infiniband-diags package to obtain the globally unique ID (GUID) through the `ibstat -p` command. See Determine host port GUIDs and make the recommended settings for information on how to install the infiniband-diags package.

Steps

1. Install the `opensm` package on any hosts that will be running the subnet manager.
2. Use the `ibstat -p` command to find `GUID0` and `GUID1` of the HCA ports. For example:

```
# ibstat -p
0x248a070300a80a80
0x248a070300a80a81
```

3. Create a subnet manager script that runs once as part of the boot process.

```
# vim /usr/sbin/subnet-manager.sh
```

4. Add the following lines. Substitute the values you found in step 2 for `GUID0` and `GUID1`. For `P0` and `P1`, use the subnet manager priorities, with 1 being the lowest and 15 the highest.

```
#!/bin/bash

opensm -B -g <GUID0> -p <P0> -f /var/log/opensm-ib0.log
opensm -B -g <GUID1> -p <P1> -f /var/log/opensm-ib1.log
```

   An example of the command with value substitutions:

```
#!/bin/bash

opensm -B -g 0x248a070300a80a80 -p 15 -f /var/log/opensm-ib0.log
opensm -B -g 0x248a070300a80a81 -p 1 -f /var/log/opensm-ib1.log
```

5. Create a systemd service unit file named `subnet-manager.service`.

```
# vim /etc/systemd/system/subnet-manager.service
```

6. Add the following lines.

```
[Unit]
Description=systemd service unit file for subnet manager

[Service]
Type=forking
ExecStart=/bin/bash /usr/sbin/subnet-manager.sh

[Install]
WantedBy=multi-user.target
```

7. Notify systemd of the new service.

```
# systemctl daemon-reload
```

8. Enable and start the `subnet-manager` service.

```
# systemctl enable subnet-manager.service
# systemctl start subnet-manager.service
```

Set up NVMe over InfiniBand on the host side

Configuring an NVMe initiator in an InfiniBand environment includes installing and configuring the infiniband, nvme-cli, and rdma packages, configuring initiator IP addresses, and setting up the NVMe-oF layer on the host.

What you'll need

You must be running the latest compatible RHEL 7, RHEL 8, RHEL9, SUSE Linux Enterprise Server 12 or 15 service pack operating system. See the NetApp Interoperability Matrix Tool for a complete list of the latest requirements.

Steps

1. Install the rdma, nvme-cli, and infiniband packages:

   SLES 12 or SLES 15

   ```
   # zypper install infiniband-diags
   # zypper install rdma-core
   # zypper install nvme-cli
   ```

   RHEL 7, RHEL 8, or RHEL 9

```
# yum install infiniband-diags
# yum install rdma-core
# yum install nvme-cli
```

2. Enable `ipoib`. Edit the /etc/rdma/rdma.conf file and modify the entry for loading `ipoib`:

```
IPOIB_LOAD=yes
```

3. Get the host NQN, which will be used to configure the host to an array.

```
# cat /etc/nvme/hostnqn
```

4. Check that both ib port links are up and the State = Active:

```
# ibstat
```

```
CA 'mlx4_0'
        CA type: MT4099
        Number of ports: 2
        Firmware version: 2.40.7000
        Hardware version: 1
        Node GUID: 0x0002c90300317850
        System image GUID: 0x0002c90300317853
        Port 1:
                State: Active
                Physical state: LinkUp
                Rate: 40
                Base lid: 4
                LMC: 0
                SM lid: 4
                Capability mask: 0x0259486a
                Port GUID: 0x0002c90300317851
                Link layer: InfiniBand
        Port 2:
                State: Active
                Physical state: LinkUp
                Rate: 56
                Base lid: 5
                LMC: 0
                SM lid: 4
                Capability mask: 0x0259486a
                Port GUID: 0x0002c90300317852
                Link layer: InfiniBand
```

5. Set up IPv4 IP addresses on the ib ports.

SLES 12 or SLES 15

Create the file /etc/sysconfig/network/ifcfg-ib0 with the following contents.

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='10.10.10.100/24'
IPOIB_MODE='connected'
MTU='65520'
NAME=
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

Then, create the file /etc/sysconfig/network/ifcfg-ib1:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='11.11.11.100/24'
IPOIB_MODE='connected'
MTU='65520'
NAME=
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

RHEL 7, RHEL 8, or RHEL 9

Create the file /etc/sysconfig/network-scripts/ifcfg-ib0 with the following contents.

```
CONNECTED_MODE=no
TYPE=InfiniBand
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR='10.10.10.100/24'
DEFROUTE=no
IPV4=FAILURE_FATAL=yes
IPV6INIT=no
NAME=ib0
ONBOOT=yes
```

Then, create the file /etc/sysconfig/network-scripts/ifcfg-ib1:

```
CONNECTED_MODE=no
TYPE=InfiniBand
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=static
IPADDR='11.11.11.100/24'
DEFROUTE=no
IPV4=FAILURE_FATAL=yes
IPV6INIT=no
NAME=ib1
ONBOOT=yes
```

6. Enable the `ib` interface:

```
# ifup ib0
# ifup ib1
```

7. Verify the IP addresses you will use to connect to the array. Run this command for both `ib0` and `ib1`:

```
# ip addr show ib0
# ip addr show ib1
```

As shown in the example below, the IP address for `ib0` is `10.10.10.255`.

```
10: ib0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 65520 qdisc pfifo_fast
state UP group default qlen 256
    link/infiniband
80:00:02:08:fe:80:00:00:00:00:00:00:02:c9:03:00:31:78:51 brd
00:ff:ff:ff:ff:12:40:1b:ff:ff:00:00:00:00:00:00:ff:ff:ff:ff
    inet 10.10.10.255 brd 10.10.10.255 scope global ib0
       valid_lft forever preferred_lft forever
    inet6 fe80::202:c903:31:7851/64 scope link
       valid_lft forever preferred_lft forever
```

As shown in the example below, the IP address for `ib1` is `11.11.11.255`.

```
10: ib1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 65520 qdisc pfifo_fast
state UP group default qlen 256
    link/infiniband
80:00:02:08:fe:80:00:00:00:00:00:00:02:c9:03:00:31:78:51 brd
00:ff:ff:ff:ff:12:40:1b:ff:ff:00:00:00:00:00:00:ff:ff:ff:ff
    inet 11.11.11.255 brd 11.11.11.255 scope global ib0
       valid_lft forever preferred_lft forever
    inet6 fe80::202:c903:31:7851/64 scope link
       valid_lft forever preferred_lft forever
```

8. Set up the NVMe-oF layer on the host. Create the following files under /etc/modules-load.d/ to load the `nvme-rdma` kernel module and make sure the kernel module will always be on, even after a reboot:

```
# cat /etc/modules-load.d/nvme-rdma.conf
  nvme-rdma
```

To verify the `nvme-rdma` kernel module is loaded, run this command:

```
# lsmod | grep nvme
nvme_rdma               36864  0
nvme_fabrics            24576  1 nvme_rdma
nvme_core              114688  5 nvme_rdma,nvme_fabrics
rdma_cm                114688  7
rpcrdma,ib_srpt,ib_srp,nvme_rdma,ib_iser,ib_isert,rdma_ucm
ib_core                393216  15
rdma_cm,ib_ipoib,rpcrdma,ib_srpt,ib_srp,nvme_rdma,iw_cm,ib_iser,ib_umad,
ib_isert,rdma_ucm,ib_uverbs,mlx5_ib,qedr,ib_cm
t10_pi                  16384  2 sd_mod,nvme_core
```

Configure storage array NVMe over InfiniBand connections

If your controller includes an NVMe over InfiniBand port, you can configure the IP address of each port using SANtricity System Manager.

Steps

1. From the System Manager interface, 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 NVMe over InfiniBand ports you want to configure.

   The controller's context menu appears.

4. Select **Configure NVMe over InfiniBand ports**.

   > The Configure NVMe over InfiniBand ports option appears only if System Manager detects NVMe over InfiniBand ports on the controller.

   The **Configure NVMe over InfiniBand Ports** dialog box opens.

5. In the drop-down list, select the HIC port you want to configure, and then enter the IP address of the port.
6. Click **Configure**.
7. Repeat steps 5 and 6 for the other HIC ports that will be used.

Discover and connect to the storage from the host

Before making definitions of each host in SANtricity System Manager, you must discover the target controller ports from the host, and then establish NVMe connections.

Steps

1. Discover available subsystems on the NVMe-oF target for all paths using the following command:

```
nvme discover -t rdma -a target_ip_address
```

In this command, `target_ip_address` is the IP address of the target port.

> The `nvme discover` command discovers all controller ports in the subsystem, regardless of host access.

```
# nvme discover -t rdma -a 10.10.10.100
 Discovery Log Number of Records 2, Generation counter 0
 =====Discovery Log Entry 0======
 trtype:  rdma
 adrfam:  ipv4
 subtype: nvme subsystem
 treq:    not specified
 portid:  0
 trsvcid: 4420
 subnqn:  nqn.1992-08.com.netapp:5700.600a098000af41580000000058ed54be
 traddr: 10.10.10.100
 rdma_prtype: infiniband
 rdma_qptype: connected
 rdma_cms:    rdma-cm
 rdma_pkey: 0x0000
=====Discovery Log Entry 1======
 trtype:  rdma
 adrfam:  ipv4
 subtype: nvme subsystem
 treq:    not specified
 portid:  1
 trsvcid: 4420
 subnqn:  nqn.1992-08.com.netapp:5700.600a098000af41580000000058ed54be
 traddr: 11.11.11.100
 rdma_prtype: infiniband
 rdma_qptype: connected
 rdma_cms:    rdma-cm
 rdma_pkey: 0x0000
```

2. Repeat step 1 for any other connections.
3. Connect to the discovered subsystem on the first path using the command: `nvme connect -t rdma -n discovered_sub_nqn -a target_ip_address -Q queue_depth_setting -l controller_loss_timeout_period`

> The above command does not persist through reboot. The `nvme connect` command will need to be executed after each reboot to re-establish the NVMe connections.

> The NVMe connections do not persist through system reboot or extended periods of the controller being unavailable.

Connections are not established for any discovered port inaccessible by the host.

If you specify a port number using this command, the connection fails. The default port is the only port set up for connections.

The recommended queue depth setting is 1024. Override the default setting of 128 with 1024 using the `-Q 1024`command line option, as shown in the following example.

The recommended controller loss timeout period in seconds is 60 minutes (3600 seconds). Override the default setting of 600 seconds with 3600 seconds using the `-l 3600` command line option, as shown in the following example:

```
# nvme connect -t rdma -a 10.10.10.100 -n nqn.1992-
08.com.netapp:5700.600a098000af41580000000058ed54be -Q 1024 -l 3600
```

4. Use the `nvme list` command to see a list of the NVMe devices currently connected. In the example below, it is `nvme0n1`.

```
 # nvme list

 Node           SN             Model              Namespace
 ------------------------------------------------------------
 /dev/nvme0n1   021648023161   NetApp E-Series       1
```

```
Usage                  Format           FW Rev
-----------------------------------------------------------------
5.37 GB /5.37 GB       512 B + 0 B      0842XXXX
```

5. Connect to the discovered subsystem on the second path:

```
  # nvme connect -t rdma -a 11.11.11.100 -n nqn.1992-
08.com.netapp:5700.600a098000af41580000000058ed54be -Q 1024 -l 3600
```

6. Use the Linux `lsblk` and `grep` commands to show additional information about each block device:

```
 # lsblk | grep nvme

 nvme0n1     259:0    0      5G  0 disk
 nvme1n1     259:0    0      5G  0 disk
```

7. Use the `nvme list` command to see a new list of the NVMe devices currently connected. In the example

below, it is `nvme0n1` and `nvme0n1`.

```
# nvme list
Node          SN            Model                    Namespace
-----------------------------------------------------------
/dev/nvme0n1  021648023161  NetApp E-Series           1
/dev/nvme1n1  021648023161  NetApp E-Series           1
```

```
Usage                  Format           FW Rev
-----------------------------------------------------------
5.37 GB /5.37 GB          512 B + 0 B      0842XXXX
5.37 GB /5.37 GB          512 B + 0 B      0842XXXX
```

Define a host

Using SANtricity System Manager, you define the hosts that send data to the storage array. Defining a host is one of the steps required to let the storage array know which hosts are attached to it and to allow I/O access to the volumes.

About this task

Keep these guidelines in mind when you define a host:

- You must define the host identifier ports that are associated with the host.
- Make sure that you provide the same name as the host's assigned system name.
- This operation does not succeed if the name you choose is already in use.
- The length of the name cannot exceed 30 characters.

Steps

1. Select **Storage › Hosts**.
2. Click **Create › Host**.

   The Create Host dialog box appears.

3. Select the settings for the host as appropriate.

Setting	Description
Name	Type a name for the new host.

Setting	Description
Host operating system type	Select one of the following options from the drop-down list: • **Linux** for SANtricity 11.60 and newer • **Linux DM-MP (Kernel 3.10 or later)** for pre-SANtricity 11.60
Host interface type	Select the host interface type that you want to use.
Host ports	Do one of the following: • **Select I/O Interface** If the host ports have logged in, you can select host port identifiers from the list. This is the recommended method. • **Manual add** If the host ports have not logged in, look at /etc/nvme/hostnqn on the host to find the hostnqn identifiers and associate them with the host definition. You can manually enter the host port identifiers or copy/paste them from the /etc/nvme/hostnqn file (one at a time) into the **Host ports** field. You must add one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the **Host ports** field. If necessary, you also can remove an identifier by selecting the **X** next to it.

4. Click **Create**.

Result

After the host is successfully created, SANtricity System Manager creates a default name for each host port configured for the host.

The default alias is `<Hostname_Port Number>`. For example, the default alias for the first port created for `host IPT is IPT_1`.

Assign a volume

You must assign a volume (namespace) to a host or host cluster so it can be used for I/O operations. This assignment grants a host or host cluster access to one or more

namespaces in a storage array.

About this task

Keep these guidelines in mind when you assign volumes:

- You can assign a volume to only one host or host cluster at a time.
- Assigned volumes are shared between controllers in the storage array.
- The same namespace ID (NSID) cannot be used twice by a host or a host cluster to access a volume. You must use a unique NSID.

Assigning a volume fails under these conditions:

- All volumes are assigned.
- The volume is already assigned to another host or host cluster.

The ability to assign a volume is unavailable under these conditions:

- No valid hosts or host clusters exist.
- All volume assignments have been defined.

All unassigned volumes are displayed, but functions for hosts with or without Data Assurance (DA) apply as follows:

- For a DA-capable host, you can select volumes that are either DA-enabled or not DA-enabled.
- For a host that is not DA-capable, if you select a volume that is DA-enabled, a warning states that the system must automatically turn off DA on the volume before assigning the volume to the host.

Steps

1. Select **Storage › Hosts**.
2. Select the host or host cluster to which you want to assign volumes, and then click **Assign Volumes**.

   A dialog box appears that lists all the volumes that can be assigned. You can sort any of the columns or type something in the **Filter** box to make it easier to find particular volumes.

3. Select the checkbox next to each volume that you want to assign or select the checkbox in the table header to select all volumes.
4. Click **Assign** to complete the operation.

Result

After successfully assigning a volume or volumes to a host or a host cluster, the system performs the following actions:

- The assigned volume receives the next available NSID. The host uses the NSID to access the volume.
- The user-supplied volume name appears in volume listings associated to the host.

Display the volumes visible to the host

You can use the SMdevices tool to view volumes currently visible on the host. This tool is part of the nvme-cli package, and can be used as an alternative to the `nvme list` command.

To view information about each NVMe path to an E-Series volume, use the `nvme netapp smdevices [-o <format>]` command. The output `<format>` can be normal (the default if -o is not used), column, or json.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Set up failover

To provide a redundant path to the storage array, you can configure the host to run failover.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`

> Refer to NetApp Interoperability Matrix Tool to ensure any required updates are installed as multipathing may not work correctly with the GA versions of SLES or RHEL.

About this task

RHEL 7 and SLES 12 use Device Mapper Multipath (DMMP) for multipathing when using NVMe over Infiniband. RHEL 8, RHEL9, and SLES 15 use a built-in Native NVMe Failover. Depending on which OS you are running, some additional configuration of multipath is required to get it running properly.

Enable Device Mapper Multipath (DMMP) for RHEL 7 or SLES 12

By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. Add the NVMe E-Series device entry to the devices section of the /etc/multipath.conf file, as shown in the following example:

```
devices {
        device {
                vendor "NVME"
                product "NetApp E-Series*"
                path_grouping_policy group_by_prio
                failback immediate
                no_path_retry 30
        }
}
```

2. Configure `multipathd` to start at system boot.

```
# systemctl enable multipathd
```

3. Start `multipathd` if it is not currently running.

```
# systemctl start multipathd
```

4. Verify the status of `multipathd` to make sure it is active and running:

```
# systemctl status multipathd
```

Setting up RHEL 8 with Native NVMe Multipathing

Native NVMe Multipathing is disabled by default in RHEL 8 and must be enabled using the steps below.

1. Setup `modprobe` rule to turn on Native NVMe Multipathing.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-
nvme_core.conf
```

2. Remake `initramfs` with new `modprobe` parameter.

```
# dracut -f
```

3. Reboot server to bring it up with the Native NVMe Multipathing enabled.

```
# reboot
```

4. Verify Native NVMe Multipathing has been enabled after the host boots back up.

```
# cat /sys/module/nvme_core/parameters/multipath
```

   a. If the command output is `N`, then Native NVMe Multipathing is still disabled.

   b. If the command output is `Y`, then Native NVMe Multipathing is enabled and any NVMe devices you discover will use it.

For SLES 15 and RHEL 9, Native NVMe Multipathing is enabled by default and no additional configuration is required.

Access NVMe volumes for virtual device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 7 and SLES 12, I/O is directed to virtual device targets by the Linux host. DM-MP manages the physical paths underlying these virtual targets.

Virtual devices are I/O targets

Make sure you are running I/O only to the virtual devices created by DM-MP and not to the physical device paths. If you are running I/O to the physical paths, DM-MP cannot manage a failover event and the I/O fails.

You can access these block devices through the `dm` device or the `symlink` in /dev/mapper. For example:

```
/dev/dm-1
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Example output

The following example output from the `nvme list` command shows the host node name and its correlation with the namespace ID.

```
NODE         SN            MODEL            NAMESPACE

/dev/nvme1n1 021648023072 NetApp E-Series 10
/dev/nvme1n2 021648023072 NetApp E-Series 11
/dev/nvme1n3 021648023072 NetApp E-Series 12
/dev/nvme1n4 021648023072 NetApp E-Series 13
/dev/nvme2n1 021648023151 NetApp E-Series 10
/dev/nvme2n2 021648023151 NetApp E-Series 11
/dev/nvme2n3 021648023151 NetApp E-Series 12
/dev/nvme2n4 021648023151 NetApp E-Series 13
```

Column	Description
`Node`	The node name includes two parts: • The notation `nvme1` represents controller A and `nvme2` represents controller B. • The notation `n1`, `n2`, and so on represent the namespace identifier from the host perspective. These identifiers are repeated in the table, once for controller A and once for controller B.
`Namespace`	The Namespace column lists the namespace ID (NSID), which is the identifier from the storage array perspective.

In the following `multipath -ll` output, the optimized paths are shown with a `prio` value of 50, while the non-optimized paths are shown with a `prio` value of 10.

The Linux operating system routes I/O to the path group that is shown as `status=active`, while the path groups listed as `status=enabled` are available for failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- #:#:#:# nvme1n1 259:5 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  `- #:#:#:# nvme2n1 259:9  active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=0 status=enabled
| `- #:#:#:# nvme1n1 259:5 failed faulty running
`-+- policy='service-time 0' prio=10 status=active
  `- #:#:#:# nvme2n1 259:9  active ready running
```

Line item	Description
`policy='service-time 0' prio=50 status=active`	This line and the following line show that `nvme1n1`, which is the namespace with an NSID of 10, is optimized on the path with a `prio` value of 50 and a `status` value of `active`. This namespace is owned by controller A.
`policy='service-time 0' prio=10 status=enabled`	This line shows the failover path for namespace 10, with a `prio` value of 10 and a `status` value of `enabled`. I/O is not being directed to the namespace on this path at the moment. This namespace is owned by controller B.
`policy='service-time 0' prio=0 status=enabled`	This example shows `multipath -ll`output from a different point in time, while controller A is rebooting. The path to namespace 10 is shown as `failed faulty running` with a `prio` value of 0 and a `status` value of `enabled`.
`policy='service-time 0' prio=10 status=active`	Note that the `active` path refers to `nvme2`, so the I/O is being directed on this path to controller B.

Access NVMe volumes for physical NVMe device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 8, RHEL 9, and SLES 15, I/O is directed to the physical NVMe device targets by the Linux host. A native NVMe multipathing solution manages the physical paths underlying the single apparent physical device displayed by the host.

Physical NVMe devices are I/O targets

It is best practice to run I/O to the links in `/dev/disk/by-id/nvme-eui.[uuid#]` rather than directly to the physical nvme device path `/dev/nvme[subsys#]n[id#]`. The link between these two locations can be found using the following command:

```
# ls /dev/disk/by-id/ -l
lrwxrwxrwx 1 root root 13 Oct 18 15:14 nvme-
eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

I/O run to `/dev/disk/by-id/nvme-eui.[uuid#]` will be passed directly through `/dev/nvme[subsys#]n[id#]` which has all paths virtualized underneath it using the Native NVMe multipathing solution.

You can view your paths by running:

```
# nvme list-subsys
```

Example output:

```
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

If you specify a physical nvme device when using the 'nvme list-subsys' command, it provides additional information about the paths to that namespace:

```
# nvme list-subsys /dev/nvme0n1
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af44620000000058d5dd96
\
 +- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
 +- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
 +- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
 +- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

There are also hooks into the multipath commands to allow you to view your path information for native failover through them as well:

```
#multipath -ll
```

To view the path information, the following must be set in /etc/multipath.conf:

```
defaults {
        enable_foreign nvme
}
```

Example output:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-
Series,08520001
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
`-+- policy='n/a' prio-10 status=non-optimized
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized    live
```

Create filesystems (RHEL 7 and SLES 12)

For RHEL 7 and SLES 12, you create a file system on the namespace and mount the filesystem.

Steps

1. Run the `multipath -ll` command to get a list of `/dev/mapper/dm` devices.

```
# multipath -ll
```

The result of this command shows two devices, `dm-19` and `dm-16`:

```
eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series
size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- #:#:#:# nvme0n19 259:19  active ready running
| `- #:#:#:# nvme1n19 259:115 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- #:#:#:# nvme2n19 259:51  active ready running
  `- #:#:#:# nvme3n19 259:83  active ready running
eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series
size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- #:#:#:# nvme0n16 259:16  active ready running
| `- #:#:#:# nvme1n16 259:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- #:#:#:# nvme2n16 259:48  active ready running
  `- #:#:#:# nvme3n16 259:80  active ready running
```

2. Create a file system on the partition for each `/dev/mapper/eui-` device.

The method for creating a file system varies depending on the file system chosen. This example shows creating an `ext4` file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Create filesystems (RHEL 8, RHEL 9, SLES 15)

For RHEL 8, RHEL 9, SLES 15, you create a filesystem on the native nvme device and mount the filesystem.

Steps

1. Run the `multipath -ll` command to get a list of nvme devices.

```
# multipath -ll
```

The result of this command can be used to find the devices associated with the `/dev/disk/by-id/nvme-eui.[uuid#]` location. For the example below, this would be `/dev/disc/by-id/nvme-eui.000082dd5c05d39300a0980000a52225`.

```
eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe,NetApp E-
Series,08520000
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=50 status=optimized
| `- 0:1:1 nvme0c1n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=10 status=non-optimized
| `- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
`-+- policy='n/a' prio=10 status=non-optimized
  `- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
```

2. Create a file system on the partition for the desired nvme device using the location `/dev/disk/by-id/nvme-eui.[id#]`.

   The method for creating a file system varies depending on the file system chosen. This example shows creating an `ext4` file system.

```
# mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
mke2fs 1.42.11 (22-Oct-2019)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verify storage access on the host

Before using the namespace, you verify that the host can write data to the namespace

and read it back.

What you'll need

An initialized namespace that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

Remove the file and folder that you copied.

Record your NVMe over IB configuration

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

Host identifiers

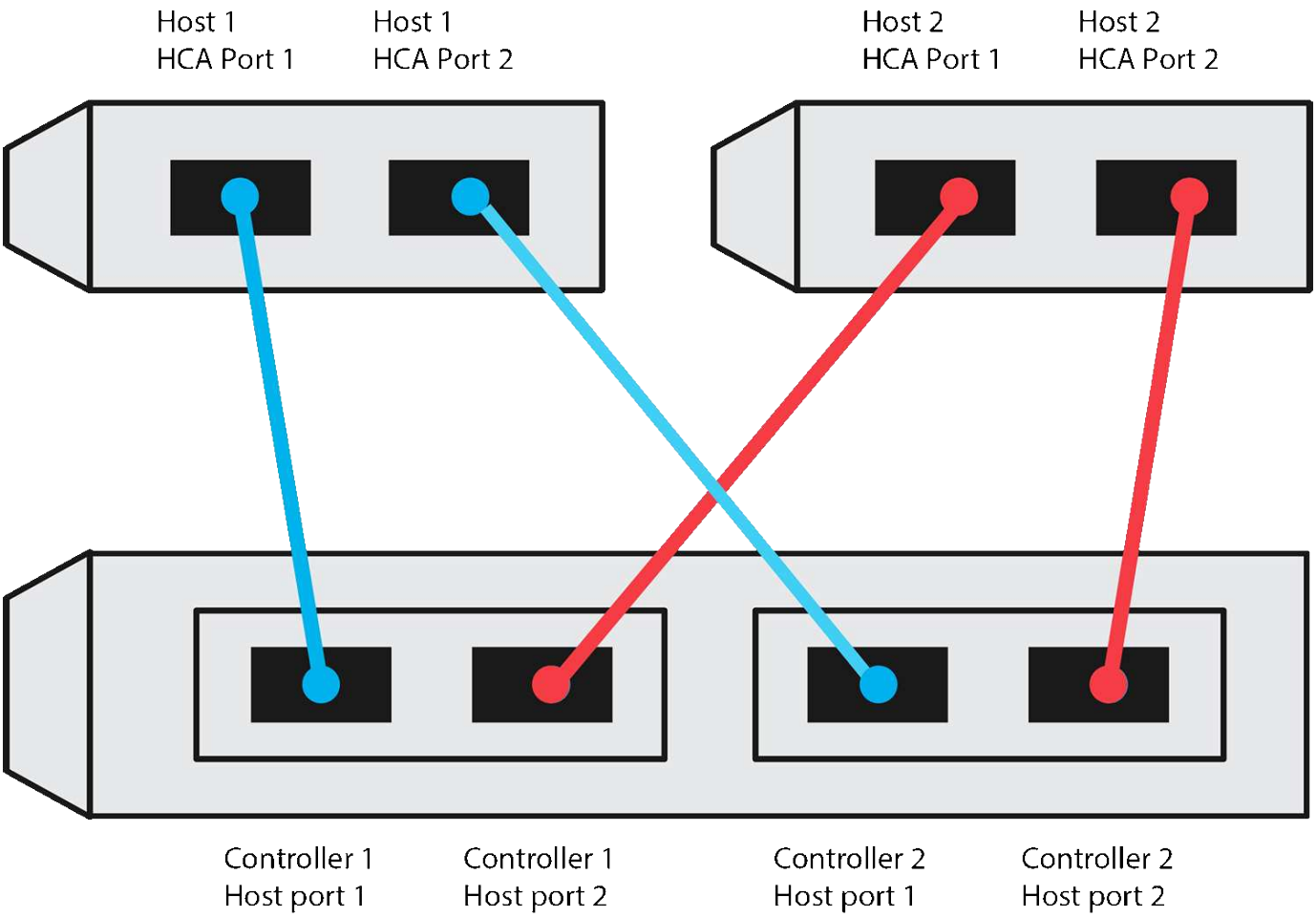
The software initiator NQN is determined during the task.

Locate and document the initiator NQN from each host. The NQN is typically found in the /etc/nvme/hostnqn file.

Callout No.	Host port connections	Host NQN
1	Host (initiator) 1	
n/a		
n/a		
n/a		
n/a		

Recommended configuration

In a direct connect topology, one or more hosts are directly connected to the subsystem. In the SANtricity OS 11.50 release, we support a single connection from each host to a subsystem controller, as shown below. In this configuration, one HCA (host channel adapter) port from each host should be on the same subnet as the E-Series controller port it is connected to, but on a different subnet from the other HCA port.



Target NQN

Document the target NQN for the storage array. You will use this information in Configure storage array NVMe over InfiniBand connections.

Find the Storage Array NQN name using SANtricity: **Storage Array** > **NVMe over Infiniband** > **Manage Settings**. This information might be necessary when you create NVMe over InfiniBand sessions from operating systems that do not support send targets discovery.

Callout No.	Array name	Target IQN
6	Array controller (target)	

Network configuration

Document the network configuration that will be used for the hosts and storage on the InfiniBand fabric. These instructions assume that two subnets will be used for full redundancy.

Your network administrator can provide the following information. You use this information in the topic, Configure storage array NVMe over InfiniBand connections.

Subnet A

Define the subnet to be used.

Network Address	Netmask

Document the NQNs to be used by the array ports and each host port.

Callout No.	Array controller (target) port connections	NQN
3	Switch	*not applicable*
5	Controller A, port 1	
4	Controller B, port 1	
2	Host 1, port 1	
	(Optional) Host 2, port 1	

Subnet B

Define the subnet to be used.

Network Address	Netmask

Document the IQNs to be used by the array ports and each host port.

Callout No.	Array controller (target) port connections	NQN
8	Switch	*not applicable*
10	Controller A, port 2	
9	Controller B, port 2	
7	Host 1, port 2	
	(Optional) Host 2, port 2	

Mapping host name

The mapping host name is created during the workflow.

Mapping host name	
Host OS type	

NVMe over RoCE Setup

Verify Linux support and review restrictions

As a first step, you should verify that your Linux configuration is supported and also review the controller, switch, host, and recovery restrictions.

Verify the Linux 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 on 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.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. 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.

Verify NVMe over RoCE restrictions

Before using NVMe over RoCE, see the NetApp Interoperability Matrix Tool to review the latest controller, host, and recovery restrictions.

Switch restrictions

RISK OF DATA LOSS. You must enable flow control for use with Global Pause Control on the switch to eliminate the risk of data loss in an NVMe over RoCE environment.

Storage and disaster recovery restrictions

- Asynchronous and synchronous mirroring are not supported.
- Thin provisioning (the creation of thin volumes) is not supported.

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.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

> If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **Disk space**: 5 GB
  - **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

Windows	Linux
Double-click the SMIA*.exe installation package to start the installation.	a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the `IATEMPDIR` variable. Example: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Run the `chmod +x SMIA*.bin` command to grant execute permission to the file. d. Run the `./SMIA*.bin` command to start the installer.

3. Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use 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

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.

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 more information, see the online help for SANtricity System Manager.

Configure the switch

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

> **RISK OF DATA LOSS.** You must enable flow control for use with Global Pause Control on the switch to eliminate the risk of data loss in an NVMe over RoCE environment.

Steps

1. Enable Ethernet pause frame flow control **end to end** as the best practice configuration.
2. Consult your network administrator for tips on selecting the best configuration for your environment.

Set up NVMe over RoCE on the host side

NVMe initiator configuration in a RoCE environment includes installing and configuring the rdma-core and nvme-cli packages, configuring initiator IP addresses, and setting up the NVMe-oF layer on the host.

What you'll need

You must be running the latest compatible RHEL 7, RHEL 8, and RHEL 9 SUSE Linux Enterprise Server 12 and 15 service pack operating system. See the NetApp Interoperability Matrix Tool for a complete list of the latest requirements.

Steps

1. Install the rdma and nvme-cli packages:

   SLES 12 or SLES 15

   ```
   # zypper install rdma-core
   # zypper install nvme-cli
   ```

   RHEL 7, RHEL 8, and RHEL 9

   ```
   # yum install rdma-core
   # yum install nvme-cli
   ```

2. Get the host NQN, which will be used to configure the host to an array.

   ```
   # cat /etc/nvme/hostnqn
   ```

3. Set up IPv4 IP addresses on the ethernet ports used to connect NVMe over RoCE. For each network interface, create a configuration script that contains the different variables for that interface.

   The variables used in this step are based on server hardware and the network environment. The variables include the `IPADDR` and `GATEWAY`. These are example instructions for SLES and RHEL:

   SLES 12 and SLES 15

   Create the example file `/etc/sysconfig/network/ifcfg-eth4` with the following contents.

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.1.87/24'
GATEWAY='192.168.1.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

   Then, create the example file `/etc/sysconfig/network/ifcfg-eth5`:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.2.87/24'
GATEWAY='192.168.2.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

   RHEL 7, RHEL 8, and RHEL 9

   Create the example file `/etc/sysconfig/network-scripts/ifcfg-eth4` with the following contents.

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.1.87/24’
GATEWAY='192.168.1.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

Then, create the example file `/etc/sysconfig/network-scripts/ifcfg-eth5`:

```
BOOTPROTO='static'
BROADCAST=
ETHTOOL_OPTIONS=
IPADDR='192.168.2.87/24'
GATEWAY='192.168.2.1'
MTU=
NAME='MT27800 Family [ConnectX-5]'
NETWORK=
REMOTE_IPADDR=
STARTMODE='auto'
```

4. Enable the network interfaces:

```
# ifup eth4
# ifup eth5
```

5. Set up the NVMe-oF layer on the host. Create the following file under `/etc/modules-load.d/` to load the `nvme-rdma` kernel module and make sure the kernel module will always be on, even after a reboot:

```
# cat /etc/modules-load.d/nvme-rdma.conf
  nvme-rdma
```

To verify the `nvme-rdma` kernel module is loaded, run this command:

```
# lsmod | grep nvme
nvme_rdma               36864  0
nvme_fabrics            24576  1 nvme_rdma
nvme_core              114688  5 nvme_rdma,nvme_fabrics
rdma_cm                114688  7
rpcrdma,ib_srpt,ib_srp,nvme_rdma,ib_iser,ib_isert,rdma_ucm
ib_core                393216  15
rdma_cm,ib_ipoib,rpcrdma,ib_srpt,ib_srp,nvme_rdma,iw_cm,ib_iser,ib_umad,
ib_isert,rdma_ucm,ib_uverbs,mlx5_ib,qedr,ib_cm
t10_pi                  16384  2 sd_mod,nvme_core
```

Configure storage array NVMe over RoCE connections

If your controller includes a connection for NVMe over RoCE (RDMA over Converged Ethernet), you can configure the NVMe port settings from the Hardware page or the System page in SANtricity System Manager.

What you'll need

- An NVMe over RoCE host port on your controller; otherwise, the NVMe over RoCE settings are not available in System Manager.
- The IP address of the host connection.

About this task

You can access the NVMe over RoCE configuration from the **Hardware** page or from **Settings › System**. This task describes how to configure the ports from the Hardware page.

> The NVMe over RoCE settings and functions appear only if your storage array's controller includes an NVMe over RoCE port.

Steps

1. From the System Manager interface, select **Hardware**.
2. Click the controller with the NVMe over RoCE port you want to configure.

   The controller's context menu appears.

3. Select **Configure NVMe over RoCE ports**.

   The **Configure NVMe over RoCE ports** dialog box opens.

4. In the drop-down list, select the port you want to configure, and then click **Next**.
5. Select the port configuration settings you want to use, 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). Possible values include: • Auto-negotiate • 10 Gbps • 25 Gbps • 40 Gbps • 50 Gbps • 100 Gbps • 200 Gbps When a 200Gb-capable HIC is attached with a QSFP56 cable, auto-negotiate is only available when you are connecting to Mellanox switches and/or adapters. The configured NVMe over RoCE port speed should match the speed capability of the SFP on the selected port. All ports must be set to the same speed.
Enable IPv4 and/or Enable IPv6	Select one or both options to enable support for IPv4 and IPv6 networks.
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 MTU size is 1500 bytes per frame. You must enter a value between 1500 and 4200.

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.

6. 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 from DHCP server	Select this option to obtain the configuration automatically.

Port setting	Description
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 addresses and router IP address. If there is only one routable IP address, set the remaining address to 0:0:0:0:0:0:0:0.
Enable VLAN support (Available by clicking **Show more settings**.)	This option is only available in an iSCSI environment. It is not available in an NVMe over RoCE environment.
Enable ethernet priority (Available by clicking **Show more settings**.)	This option is only available in an iSCSI environment. It is not available in an NVMe over RoCE environment.

7. Click **Finish**.

Discover and connect to the storage from the host

Before making definitions of each host in SANtricity System Manager, you must discover the target controller ports from the host, and then establish NVMe connections.

Steps

1. Discover available subsystems on the NVMe-oF target for all paths using the following command:

```
nvme discover -t rdma -a target_ip_address
```

In this command, `target_ip_address` is the IP address of the target port.

The `nvme discover` command discovers all controller ports in the subsystem, regardless of host access.

```
# nvme discover -t rdma -a 192.168.1.77
Discovery Log Number of Records 2, Generation counter 0
=====Discovery Log Entry 0======
trtype:  rdma
adrfam:  ipv4
subtype: nvme subsystem
treq:    not specified
portid:  0
trsvcid: 4420
subnqn:  nqn.1992-08.com.netapp:5700.600a098000a527a7000000005ab3af94
traddr:  192.168.1.77
rdma_prtype: roce
rdma_qptype: connected
rdma_cms:    rdma-cm
rdma_pkey: 0x0000
=====Discovery Log Entry 1======
trtype:  rdma
adrfam:  ipv4
subtype: nvme subsystem
treq:    not specified
portid:  1
trsvcid: 4420
subnqn:  nqn.1992-08.com.netapp:5700.600a098000a527a7000000005ab3af94
traddr:  192.168.2.77
rdma_prtype: roce
rdma_qptype: connected
rdma_cms:    rdma-cm
rdma_pkey: 0x0000
```

2. Repeat step 1 for any other connections.
3. Connect to the discovered subsystem on the first path using the command: `nvme connect -t rdma -n discovered_sub_nqn -a target_ip_address -Q queue_depth_setting -l controller_loss_timeout_period`

> The command listed above does not persist through reboot. The `NVMe connect` command will need to be executed after each reboot to re-establish the NVMe connections.

> Connections are not established for any discovered port inaccessible by the host.

> If you specify a port number using this command, the connection fails. The default port is the only port set up for connections.

> The recommended queue depth setting is 1024. Override the default setting of 128 with 1024 using the `-Q 1024`command line option, as shown in the following example.

The recommended controller loss timeout period in seconds is 60 minutes (3600 seconds). Override the default setting of 600 seconds with 3600 seconds using the `-l 3600` command line option, as shown in the following example.

```
# nvme connect -t rdma -a 192.168.1.77 -n nqn.1992-
08.com.netapp:5700.600a098000a527a7000000005ab3af94 -Q 1024 -l 3600
# nvme connect -t rdma -a 192.168.2.77 -n nqn.1992-
08.com.netapp:5700.600a098000a527a7000000005ab3af94 -Q 1024 -l 3600
```

4. Repeat step 3 to connect the discovered subsystem on the second path.

Define a host

Using SANtricity System Manager, you define the hosts that send data to the storage array. Defining a host is one of the steps required to let the storage array know which hosts are attached to it and to allow I/O access to the volumes.

About this task

Keep these guidelines in mind when you define a host:

- You must define the host identifier ports that are associated with the host.
- Make sure that you provide the same name as the host's assigned system name.
- This operation does not succeed if the name you choose is already in use.
- The length of the name cannot exceed 30 characters.

Steps

1. Select **Storage › Hosts**.
2. Click **Create › Host**.

   The Create Host dialog box appears.

3. Select the settings for the host as appropriate.

Setting	Description
Name	Type a name for the new host.
Host operating system type	Select one of the following options from the drop-down list: • **Linux** for SANtricity 11.60 and newer • **Linux DM-MP (Kernel 3.10 or later)** for pre-SANtricity 11.60

Setting	Description
Host interface type	Select the host interface type that you want to use. If the array you configure only has one available host interface type, this setting may not be available to select.
Host ports	Do one of the following: • **Select I/O Interface** If the host ports have logged in, you can select host port identifiers from the list. This is the recommended method. • **Manual add** If the host ports have not logged in, look at /etc/nvme/hostnqn on the host to find the hostnqn identifiers and associate them with the host definition. You can manually enter the host port identifiers or copy/paste them from the /etc/nvme/hostnqn file (one at a time) into the **Host ports** field. You must add one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the **Host ports** field. If necessary, you also can remove an identifier by selecting the **X** next to it.

4. Click **Create**.

Result

After the host is successfully created, SANtricity System Manager creates a default name for each host port configured for the host.

The default alias is `<Hostname_Port Number>`. For example, the default alias for the first port created for `host IPT is IPT_1`.

Assign a volume

You must assign a volume (namespace) to a host or host cluster so it can be used for I/O operations. This assignment grants a host or host cluster access to one or more namespaces in a storage array.

About this task

Keep these guidelines in mind when you assign volumes:

- You can assign a volume to only one host or host cluster at a time.
- Assigned volumes are shared between controllers in the storage array.
- The same namespace ID (NSID) cannot be used twice by a host or a host cluster to access a volume. You must use a unique NSID.

Assigning a volume fails under these conditions:

- All volumes are assigned.
- The volume is already assigned to another host or host cluster.

The ability to assign a volume is unavailable under these conditions:

- No valid hosts or host clusters exist.
- All volume assignments have been defined.

All unassigned volumes are displayed, but functions for hosts with or without Data Assurance (DA) apply as follows:

- For a DA-capable host, you can select volumes that are either DA-enabled or not DA-enabled.
- For a host that is not DA-capable, if you select a volume that is DA-enabled, a warning states that the system must automatically turn off DA on the volume before assigning the volume to the host.

Steps

1. Select **Storage › Hosts**.
2. Select the host or host cluster to which you want to assign volumes, and then click **Assign Volumes**.

   A dialog box appears that lists all the volumes that can be assigned. You can sort any of the columns or type something in the **Filter** box to make it easier to find particular volumes.

3. Select the checkbox next to each volume that you want to assign or select the checkbox in the table header to select all volumes.
4. Click **Assign** to complete the operation.

Result

After successfully assigning a volume or volumes to a host or a host cluster, the system performs the following actions:

- The assigned volume receives the next available NSID. The host uses the NSID to access the volume.
- The user-supplied volume name appears in volume listings associated to the host.

Display the volumes visible to the host

You can use the SMdevices tool to view volumes currently visible on the host. This tool is part of the nvme-cli package, and can be used as an alternative to the `nvme list` command.

To view information about each NVMe path to an E-Series volume, use the `nvme netapp smdevices [-o <format>]` command. The output <format> can be normal (the default if -o is not used), column, or json.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Set up failover on the host

To provide a redundant path to the storage array, you can configure the host to run failover.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`

> Refer to the NetApp Interoperability Matrix Tool to ensure any required updates are installed, as multipathing might not work correctly with the GA versions of SLES or RHEL.

About this task

RHEL 7 and SLES 12 use Device Mapper Multipath (DMMP) for multipathing for NVMe over RoCE. RHEL 8, RHEL 9, and SLES 15 use a built-in Native NVMe Failover. Depending on which OS you are running, some additional configuration of multipath is required to get it running properly.

Enable Device Mapper Multipath (DMMP) for RHEL 7 or SLES 12

By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. Add the NVMe E-Series device entry to the devices section of the `/etc/multipath.conf` file, as shown in the following example:

```
devices {
        device {
                vendor "NVME"
                product "NetApp E-Series*"
                path_grouping_policy group_by_prio
                failback immediate
                no_path_retry 30
        }
}
```

2. Configure `multipathd` to start at system boot.

```
# systemctl enable multipathd
```

3. Start `multipathd` if it is not currently running.

```
# systemctl start multipathd
```

4. Verify the status of `multipathd` to make sure it is active and running:

```
# systemctl status multipathd
```

Set up RHEL 8 with Native NVMe Multipathing

Native NVMe Multipathing is disabled by default in RHEL 8 and must be enabled using the following procedure.

1. Set up the `modprobe` rule to turn on Native NVMe Multipathing.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-
nvme_core.conf
```

2. Remake `initramfs` with the new `modprobe` parameter.

```
# dracut -f
```

3. Reboot the server to bring it up with the Native NVMe Multipathing enabled.

```
# reboot
```

4. Verify that Native NVMe Multipathing is enabled after the host boots back up.

```
# cat /sys/module/nvme_core/parameters/multipath
```

   a. If the command output is `N`, then Native NVMe Multipathing is still disabled.

   b. If the command output is `Y`, then Native NVMe Multipathing is enabled and any NVMe devices you discover will use it.

For RHEL 9 and SLES 15, Native NVMe Multipathing is enabled by default and no additional configuration is required.

Access NVMe volumes for virtual device targets

You can configure the I/O that is directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 7 and SLES 12, I/O is directed to virtual device targets by the Linux host. DM-MP manages the physical paths underlying these virtual targets.

Virtual devices are I/O targets

Make sure you are running I/O only to the virtual devices created by DM-MP and not to the physical device paths. If you are running I/O to the physical paths, DM-MP cannot manage a failover event and the I/O fails.

You can access these block devices through the `dm` device or the `symlink` in /dev/mapper. For example:

```
/dev/dm-1
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Example

The following example output from the `nvme list` command shows the host node name and its correlation with the namespace ID.

```
NODE         SN           MODEL            NAMESPACE

/dev/nvme1n1 021648023072 NetApp E-Series 10
/dev/nvme1n2 021648023072 NetApp E-Series 11
/dev/nvme1n3 021648023072 NetApp E-Series 12
/dev/nvme1n4 021648023072 NetApp E-Series 13
/dev/nvme2n1 021648023151 NetApp E-Series 10
/dev/nvme2n2 021648023151 NetApp E-Series 11
/dev/nvme2n3 021648023151 NetApp E-Series 12
/dev/nvme2n4 021648023151 NetApp E-Series 13
```

Column	Description
`Node`	The node name includes two parts: • The notation `nvme1` represents controller A and `nvme2` represents controller B. • The notation `n1`, `n2`, and so on represent the namespace identifier from the host perspective. These identifiers are repeated in the table, once for controller A and once for controller B.
`Namespace`	The Namespace column lists the namespace ID (NSID), which is the identifier from the storage array perspective.

In the following `multipath -ll` output, the optimized paths are shown with a `prio` value of 50, while the non-optimized paths are shown with a `prio` value of 10.

The Linux operating system routes I/O to the path group that is shown as `status=active`, while the path groups listed as `status=enabled` are available for failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- #:#:#:# nvme1n1 259:5 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  `- #:#:#:# nvme2n1 259:9  active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=0 status=enabled
| `- #:#:#:# nvme1n1 259:5 failed faulty running
`-+- policy='service-time 0' prio=10 status=active
  `- #:#:#:# nvme2n1 259:9  active ready running
```

Line item	Description
`policy='service-time 0' prio=50 status=active`	This line and the following line show that `nvme1n1`, which is the namespace with an NSID of 10, is optimized on the path with a `prio` value of 50 and a `status` value of `active`. This namespace is owned by controller A.
`policy='service-time 0' prio=10 status=enabled`	This line shows the failover path for namespace 10, with a `prio` value of 10 and a `status` value of `enabled`. I/O is not being directed to the namespace on this path at the moment. This namespace is owned by controller B.
`policy='service-time 0' prio=0 status=enabled`	This example shows `multipath -ll`output from a different point in time, while controller A is rebooting. The path to namespace 10 is shown as `failed faulty running` with a `prio` value of 0 and a `status` value of `enabled`.
`policy='service-time 0' prio=10 status=active`	Note that the `active` path refers to `nvme2`, so the I/O is being directed on this path to controller B.

Accessing NVMe volumes for physical NVMe device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 8, RHEL 9, and SLES 15, I/O is directed to the physical NVMe device targets by the Linux host. A native NVMe multipathing solution manages the physical paths underlying the single apparent physical device displayed by the host.

Physical NVMe devices are I/O targets

It is best practice to run I/O to the links in `/dev/disk/by-id/nvme-eui.[uuid#]` rather than directly to the physical nvme device path `/dev/nvme[subsys#]n[id#]`. The link between these two locations can be found using the following command:

```
# ls /dev/disk/by-id/ -l
lrwxrwxrwx 1 root root 13 Oct 18 15:14 nvme-
eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

I/O run to `/dev/disk/by-id/nvme-eui.[uuid#]` will be passed directly through `/dev/nvme[subsys#]n[id#]` which has all paths virtualized underneath it using the Native NVMe multipathing solution.

You can view your paths by running:

```
# nvme list-subsys
```

Example output:

```
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

If you specify a namespace device when using the `nvme list-subsys` command, it provides additional information about the paths to that namespace:

```
# nvme list-subsys /dev/nvme0n1
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af44620000000058d5dd96
\
 +- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
 +- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
 +- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
 +- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

There are also hooks into the multipath commands to allow you to view your path information for native failover through them as well:

```
#multipath -ll
```

To view the path information, the following must be set in /etc/multipath.conf:

```
defaults {
        enable_foreign nvme
}
```

Example output:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-
Series,08520001
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
`-+- policy='n/a' prio-10 status=non-optimized
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized    live
```

Create filesystems (RHEL 7 and SLES 12)

For RHEL 7 and SLES 12, you create a file system on the namespace and mount the filesystem.

Steps

1. Run the `multipath -ll` command to get a list of `/dev/mapper/dm` devices.

   ```
   # multipath -ll
   ```

   The result of this command shows two devices, `dm-19` and `dm-16`:

   ```
   eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series
   size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='service-time 0' prio=50 status=active
   | |- #:#:#:# nvme0n19 259:19  active ready running
   | `- #:#:#:# nvme1n19 259:115 active ready running
   `-+- policy='service-time 0' prio=10 status=enabled
     |- #:#:#:# nvme2n19 259:51  active ready running
     `- #:#:#:# nvme3n19 259:83  active ready running
   eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series
   size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='service-time 0' prio=50 status=active
   | |- #:#:#:# nvme0n16 259:16  active ready running
   | `- #:#:#:# nvme1n16 259:112 active ready running
   `-+- policy='service-time 0' prio=10 status=enabled
     |- #:#:#:# nvme2n16 259:48  active ready running
     `- #:#:#:# nvme3n16 259:80  active ready running
   ```

2. Create a file system on the partition for each `/dev/mapper/eui-` device.

   The method for creating a file system varies depending on the file system chosen. This example shows creating an `ext4` file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Create filesystems (RHEL 8, RHEL 9, and SLES 15)

For RHEL 8, RHEL 9, and SLES 15, you create a filesystem on the native nvme device and mount the filesystem.

Steps

1. Run the `multipath -ll` command to get a list of nvme devices.

```
# multipath -ll
```

The result of this command can be used to find the devices associated `/dev/disk/by-id/nvme-eui.[uuid#]` location. For the example below this would be `/dev/disc/by-id/nvme-eui.000082dd5c05d39300a0980000a52225`.

```
eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe,NetApp E-
Series,08520000
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=50 status=optimized
| `- 0:1:1 nvme0c1n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=10 status=non-optimized
| `- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
`-+- policy='n/a' prio=10 status=non-optimized
  `- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
```

2. Create a file system on the partition for the desired nvme device using the location `/dev/disk/by-id/nvme-eui.[id#]`.

   The method for creating a file system varies depending on the file system chosen. This example shows creating an `ext4` file system.

```
# mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
mke2fs 1.42.11 (22-Oct-2019)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verify storage access on the host

Before using the namespace, verify that the host can write data to the namespace and

read it back.

What you'll need

An initialized namespace that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the `diff` command to compare the copied files to the originals.

After you finish

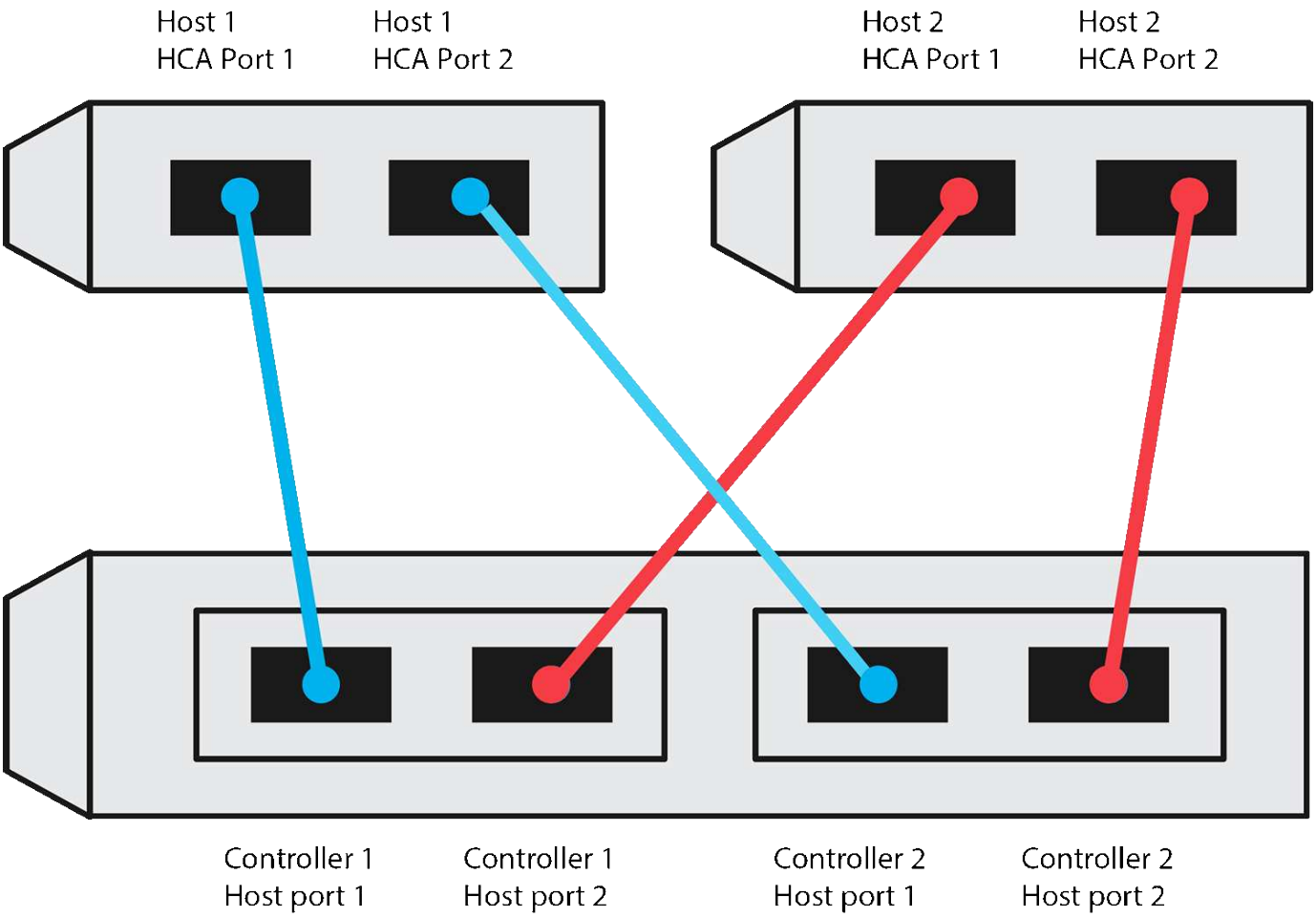
You remove the file and folder that you copied.

Record your NVMe over RoCE configuration

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

Direct connect topology

In a direct connect topology, one or more hosts are directly connected to the subsystem. In the SANtricity OS 11.50 release, we support a single connection from each host to a subsystem controller, as shown below. In this configuration, one HCA (host channel adapter) port from each host should be on the same subnet as the E-Series controller port it is connected to, but on a different subnet from the other HCA port.

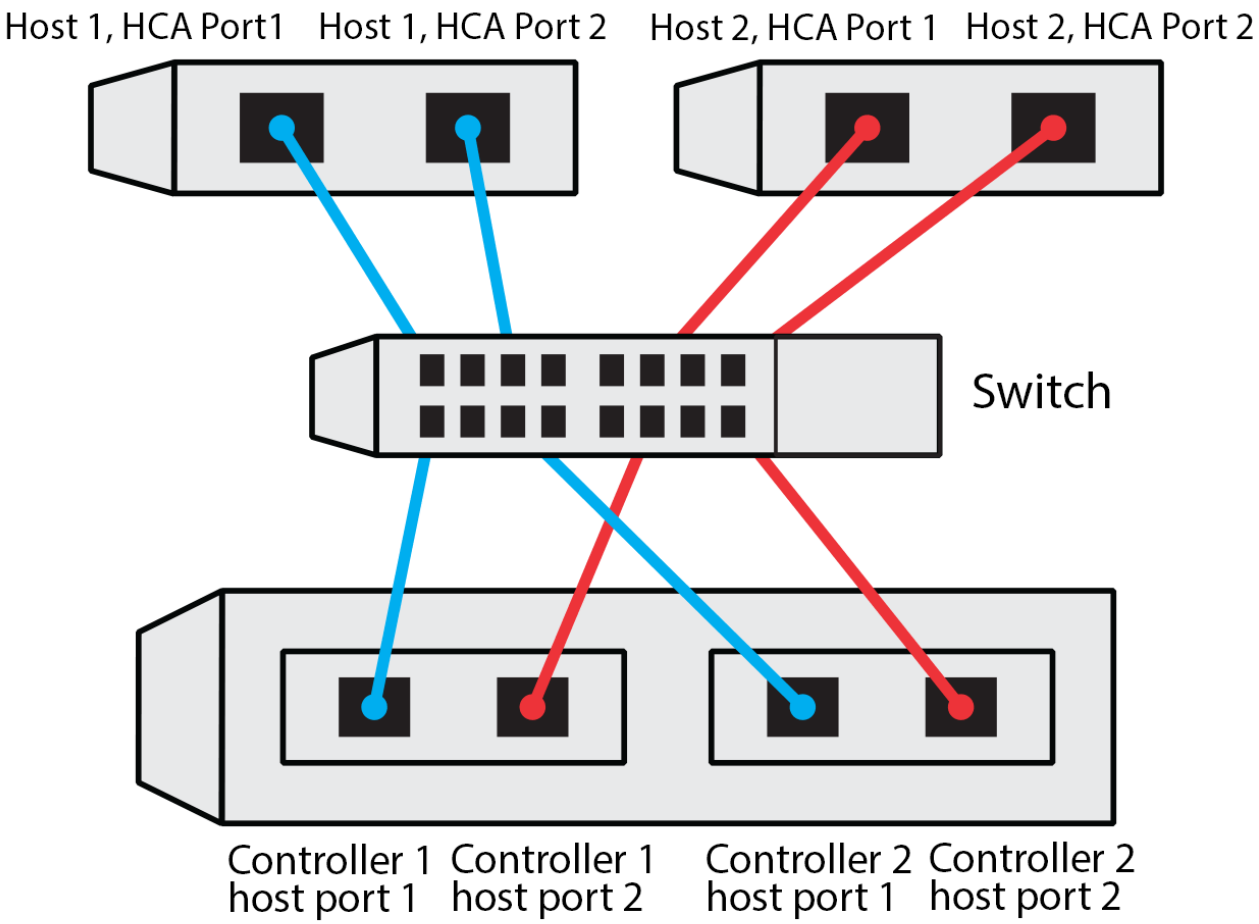


An example configuration that satisfies the requirements consists of four network subnets as follows:

- Subnet 1: Host 1 HCA Port 1 and Controller 1 Host port 1
- Subnet 2: Host 1 HCA Port 2 and Controller 2 Host port 1
- Subnet 3: Host 2 HCA Port 1 and Controller 1 Host port 2
- Subnet 4: Host 2 HCA Port 2 and Controller 2 Host port 2

Switch connect topology

In a fabric topology, one or more switches are used. Refer to NetApp Interoperability Matrix Tool for a list of supported switches.



Host identifiers

Locate and document the initiator NQN from each host.

Host port connections	Software initiator NQN
Host (initiator) 1	
Host (initiator) 2	

Target NQN

Document the target NQN for the storage array.

Array name	Target NQN
Array controller (target)	

Target NQNs

Document the NQNs to be used by the array ports.

Array controller (target) port connections	NQN
Controller A, port 1	
Controller B, port 1	
Controller A, port 2	
Controller B, port 2	

Mapping host name

The mapping host name is created during the workflow.

Mapping host name	
Host OS type	

NVMe over Fibre Channel setup

Verify Linux support and review restrictions

As a first step, you should verify that your Linux configuration is supported and also review the controller, host, and recovery restrictions.

Verify the Linux 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 on 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.

5. Select the criteria you know you want for your configuration, and then see what compatible configuration elements apply.
6. 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.

Review restrictions for NVMe over FC

Before using NVMe over Fibre Channel, see the NetApp Interoperability Matrix Tool to review the latest controller, host, and recovery restrictions.

Storage and disaster recovery restrictions

- Asynchronous and synchronous mirroring are not supported.
- Thin provisioning (the creation of thin volumes) is not supported.

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.

Install SANtricity Storage Manager for SMcli (SANtricity software version 11.53 or earlier)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- Correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client with the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **Disk space**: 5 GB
  - **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

About this task

This task describes how to install SANtricity Storage Manager on both the Windows and Linux OS platforms, because both Windows and Linux are common management station platforms when Linux is used for the data host.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer.

Windows	Linux
Double-click the SMIA*.exe installation package to start the installation.	a. Go to the directory where the SMIA*.bin installation package is located. b. If the temp mount point does not have execute permissions, set the `IATEMPDIR` variable. Example: `IATEMPDIR=/root ./SMIA-LINUXX64-11.25.0A00.0002.bin` c. Run the `chmod +x SMIA*.bin` command to grant execute permission to the file. d. Run the `./SMIA*.bin` command to start the installer.

3. Use the installation wizard to install the software on the management station.

Access SANtricity System Manager and use 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

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.

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 more information, see the online help for SANtricity System Manager.

Configure the FC switches

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.)

About this task

For details about zoning your switches, see the switch vendor's documentation.

Each initiator port must be in a separate zone with all of its corresponding target ports.

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.

Set up NVMe over Fibre Channel on the host side

NVMe initiator configuration in a Fibre Channel environment includes installing and configuring the nvme-cli package and for enabling the NVMe/FC initiator on the host.

About this task

The following procedure is for RHEL 7, RHEL 8, RHEL 9, SLES 12, and SLES 15 using Broadcom Emulex or QLogic NVMe/FC capable FC HBAs. For more information on which versions of these OS's or HBA's are supported, consult the NetApp Interoperability Matrix Tool.

Steps

1. Install the `nvme-cli` package:

   SLES 12 or SLES 15

   ```
   # zypper install nvme-cli
   ```

   RHEL 7, RHEL 8 or RHEL 9

   ```
   # yum install nvme-cli
   ```

   a. For RHEL 7 only, download and install an external Broadcom Autoconnect script for NVMe/FC connections through the Broadcom website. Enter the keyword **Autoconnect Script File for Inbox NVMe over FC Drivers** and choose the latest version specific to your OS.

   b. For Qlogic, modify `/lib/systemd/system/nvmefc-boot-connections.service` after installing the Broadcom NVMe/FC autoconnect script to contain the following:

```
[Unit]
Description=Auto-connect to subsystems on FC-NVME devices found
during boot

[Service]
Type=oneshot
ExecStart=/bin/sh -c "echo add >
/sys/class/fc/fc_udev_device/nvme_discovery"

[Install]
WantedBy=default.target
```

2. Enable and start the `nvmefc-boot-connections` service.

```
systemctl enable nvmefc-boot-connections.service
```

```
systemctl start nvmefc-boot-connections.service
```

Host-side setup for Emulex HBAs:

The following steps are for Emulex HBAs only.

1. Set `lpfc_enable_fc4_type` to `3` to enable SLES12 SP4 as an NVMe/FC initiator.

```
# cat /etc/modprobe.d/lpfc.conf
options lpfc lpfc_enable_fc4_type=3
```

2. Re-build the `initrd` to get the Emulex change and the boot parameter change.

```
# dracut --force
```

3. Reboot the host to load the changes to the `lpfc` driver.

```
# reboot
```

The host is rebooted and the NVMe/FC initiator is enabled on the host.

After completing the host-side setup, connection of the NVMe over Fibre Channel ports occur automatically.

Define a host

Using SANtricity System Manager, you define the hosts that send data to the storage array. Defining a host is one of the steps required to let the storage array know which hosts are attached to it and to allow I/O access to the volumes.

About this task

Keep these guidelines in mind when you define a host:

- You must define the host identifier ports that are associated with the host.
- Make sure that you provide the same name as the host's assigned system name.
- This operation does not succeed if the name you choose is already in use.
- The length of the name cannot exceed 30 characters.

Steps

1. Select **Storage › Hosts**.
2. Click **Create › Host**.

   The Create Host dialog box appears.

3. Select the settings for the host as appropriate.

Setting	Description
Name	Type a name for the new host.
Host operating system type	Select one of the following options from the drop-down list: • **Linux** for SANtricity 11.60 and newer • **Linux DM-MP (Kernel 3.10 or later)** for pre-SANtricity 11.60
Host interface type	Select the host interface type that you want to use. If the array you configure only has one available host interface type, this setting might not be available to select.

Setting	Description
Host ports	Do one of the following: • **Select I/O Interface** If the host ports have logged in, you can select host port identifiers from the list. This is the recommended method. • **Manual add** If the host ports have not logged in, look at /etc/nvme/hostnqn on the host to find the hostnqn identifiers and associate them with the host definition. You can manually enter the host port identifiers or copy/paste them from the /etc/nvme/hostnqn file (one at a time) into the **Host ports** field. You must add one host port identifier at a time to associate it with the host, but you can continue to select as many identifiers that are associated with the host. Each identifier is displayed in the **Host ports** field. If necessary, you also can remove an identifier by selecting the **X** next to it.

4. Click **Create**.

Result

After the host is successfully created, SANtricity System Manager creates a default name for each host port configured for the host.

The default alias is `<Hostname_Port Number>`. For example, the default alias for the first port created for `host IPT is IPT_1`.

Assign a volume

You must assign a volume (namespace) to a host or host cluster so it can be used for I/O operations. This assignment grants a host or host cluster access to one or more namespaces in a storage array.

About this task

Keep these guidelines in mind when you assign volumes:

- You can assign a volume to only one host or host cluster at a time.
- Assigned volumes are shared between controllers in the storage array.
- The same namespace ID (NSID) cannot be used twice by a host or a host cluster to access a volume. You must use a unique NSID.

Assigning a volume fails under these conditions:

- All volumes are assigned.
- The volume is already assigned to another host or host cluster.

The ability to assign a volume is unavailable under these conditions:

- No valid hosts or host clusters exist.
- All volume assignments have been defined.

All unassigned volumes are displayed, but functions for hosts with or without Data Assurance (DA) apply as follows:

- For a DA-capable host, you can select volumes that are either DA-enabled or not DA-enabled.
- For a host that is not DA-capable, if you select a volume that is DA-enabled, a warning states that the system must automatically turn off DA on the volume before assigning the volume to the host.

Steps

1. Select **Storage › Hosts**.
2. Select the host or host cluster to which you want to assign volumes, and then click **Assign Volumes**.

   A dialog box appears that lists all the volumes that can be assigned. You can sort any of the columns or type something in the **Filter** box to make it easier to find particular volumes.

3. Select the checkbox next to each volume that you want to assign or select the checkbox in the table header to select all volumes.
4. Click **Assign** to complete the operation.

Result

After successfully assigning a volume or volumes to a host or a host cluster, the system performs the following actions:

- The assigned volume receives the next available NSID. The host uses the NSID to access the volume.
- The user-supplied volume name appears in volume listings associated to the host.

Display the volumes visible to the host

You can use the SMdevices tool to view volumes currently visible on the host. This tool is part of the nvme-cli package, and can be used as an alternative to the `nvme list` command.

To view information about each NVMe path to an E-Series volume, use the `nvme netapp smdevices [-o <format>]` command.

The output `<format>` can be normal (the default if -o is not used), column, or json.

```
# nvme netapp smdevices
/dev/nvme1n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller A, Access State unknown,
2.15GB
/dev/nvme1n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller A, Access State unknown,
2.15GB
/dev/nvme2n1, Array Name ICTM0706SYS04, Volume Name NVMe2, NSID 1, Volume
ID 000015bd5903df4a00a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n2, Array Name ICTM0706SYS04, Volume Name NVMe3, NSID 2, Volume
ID 000015c05903e24000a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n3, Array Name ICTM0706SYS04, Volume Name NVMe4, NSID 4, Volume
ID 00001bb0593a46f400a0980000af4462, Controller B, Access State unknown,
2.15GB
/dev/nvme2n4, Array Name ICTM0706SYS04, Volume Name NVMe6, NSID 6, Volume
ID 00001696593b424b00a0980000af4112, Controller B, Access State unknown,
2.15GB
```

Set up failover on the host

To provide a redundant path to the storage array, you can configure the host to run failover.

What you'll need

You must install the required packages on your system.

- For Red Hat (RHEL) hosts, verify the packages are installed by running `rpm -q device-mapper-multipath`
- For SLES hosts, verify the packages are installed by running `rpm -q multipath-tools`

About this task

RHEL 7 and SLES 12 use Device Mapper Multipath (DMMP) for multipathing when using NVMe over Fibre Channel. RHEL 8, RHEL 9, and SLES 15 use a built-in Native NVMe Failover. Depending on which OS you are running, some additional configuration of multipath is required to get it running properly.

Enable Device Mapper Multipath (DMMP) for RHEL 7 or SLES 12

By default, DM-MP is disabled in RHEL and SLES. Complete the following steps to enable DM-MP components on the host.

Steps

1. Add the NVMe E-Series device entry to the devices section of the /etc/multipath.conf file, as shown in the following example:

```
devices {
        device {
                vendor "NVME"
                product "NetApp E-Series*"
                path_grouping_policy group_by_prio
                failback immediate
                no_path_retry 30
        }
}
```

2. Configure `multipathd` to start at system boot.

```
# systemctl enable multipathd
```

3. Start `multipathd` if it is not currently running.

```
# systemctl start multipathd
```

4. Verify the status of `multipathd` to make sure it is active and running:

```
# systemctl status multipathd
```

Set up Native NVMe Multipathing for RHEL 8

About this task

Native NVMe Multipathing is disabled by default in RHEL 8 and must be enabled using the steps below.

Steps

1. Setup `modprobe` rule to turn on Native NVMe Multipathing.

```
# echo "options nvme_core multipath=y" >> /etc/modprobe.d/50-
nvme_core.conf
```

2. Remake `initramfs` with new modprobe parameter.

```
# dracut -f
```

3. Reboot server to bring it up with the Native NVMe Multipathing enabled

```
# reboot
```

4. Verify Native NVMe Multipathing has been enabled after the host boots back up.

```
# cat /sys/module/nvme_core/parameters/multipath
```

   a. If the command output is `N`, then Native NVMe Multipathing is still disabled.

   b. If the command output is `Y`, then Native NVMe Multipathing is enabled and any NVMe devices you discover will use it.

For RHEL 9 and SLES 15, Native NVMe Multipathing is enabled by default and no additional configuration is required.

Access NVMe volumes for virtual device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 7 and SLES 12, I/O is directed to virtual device targets by the Linux host. DM-MP manages the physical paths underlying these virtual targets.

Virtual devices are I/O targets

Make sure you are running I/O only to the virtual devices created by DM-MP and not to the physical device paths. If you are running I/O to the physical paths, DM-MP cannot manage a failover event and the I/O fails.

You can access these block devices through the `dm` device or the `symlink` in `/dev/mapper`; for example:

```
/dev/dm-1
/dev/mapper/eui.00001bc7593b7f5f00a0980000af4462
```

Example

The following example output from the `nvme list` command shows the host node name and its correlation with the namespace ID.

```
NODE         SN           MODEL            NAMESPACE

/dev/nvme1n1 021648023072 NetApp E-Series 10
/dev/nvme1n2 021648023072 NetApp E-Series 11
/dev/nvme1n3 021648023072 NetApp E-Series 12
/dev/nvme1n4 021648023072 NetApp E-Series 13
/dev/nvme2n1 021648023151 NetApp E-Series 10
/dev/nvme2n2 021648023151 NetApp E-Series 11
/dev/nvme2n3 021648023151 NetApp E-Series 12
/dev/nvme2n4 021648023151 NetApp E-Series 13
```

Column	Description
`Node`	The node name includes two parts: • The notation `nvme1` represents controller A and `nvme2` represents controller B. • The notation `n1`, `n2`, and so on represent the namespace identifier from the host perspective. These identifiers are repeated in the table, once for controller A and once for controller B.
`Namespace`	The Namespace column lists the namespace ID (NSID), which is the identifier from the storage array perspective.

In the following `multipath -ll` output, the optimized paths are shown with a `prio` value of 50, while the non-optimized paths are shown with a `prio` value of 10.

The Linux operating system routes I/O to the path group that is shown as `status=active`, while the path groups listed as `status=enabled` are available for failover.

```
eui.00001bc7593b7f500a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- #:#:#:# nvme1n1 259:5 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  `- #:#:#:# nvme2n1 259:9  active ready running

eui.00001bc7593b7f5f00a0980000af4462 dm-0 NVME,NetApp E-Series
size=15G features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=0 status=enabled
| `- #:#:#:# nvme1n1 259:5 failed faulty running
`-+- policy='service-time 0' prio=10 status=active
  `- #:#:#:# nvme2n1 259:9  active ready running
```

Line item	Description
`policy='service-time 0' prio=50 status=active`	This line and the following line show that `nvme1n1`, which is the namespace with an NSID of 10, is optimized on the path with a `prio` value of 50 and a `status` value of `active`. This namespace is owned by controller A.
`policy='service-time 0' prio=10 status=enabled`	This line shows the failover path for namespace 10, with a `prio` value of 10 and a `status` value of `enabled`. I/O is not being directed to the namespace on this path at the moment. This namespace is owned by controller B.
`policy='service-time 0' prio=0 status=enabled`	This example shows `multipath -ll`output from a different point in time, while controller A is rebooting. The path to namespace 10 is shown as `failed faulty running` with a `prio` value of 0 and a `status` value of `enabled`.
`policy='service-time 0' prio=10 status=active`	Note that the `active` path refers to `nvme2`, so the I/O is being directed on this path to controller B.

Access NVMe volumes for physical NVMe device targets

You can configure the I/O directed to the device target based on which OS (and by extension multipathing method) you are using.

For RHEL 8, RHEL 9, and SLES 15, I/O is directed to the physical NVMe device targets by the Linux host. A native NVMe multipathing solution manages the physical paths underlying the single apparent physical device displayed by the host.

Physical NVMe devices are I/O targets

It is best practice to run I/O to the links in `/dev/disk/by-id/nvme-eui.[uuid#]` rather than directly to the physical nvme device path `/dev/nvme[subsys#]n[id#]`. The link between these two locations can be found using the following command:

```
# ls /dev/disk/by-id/ -l
lrwxrwxrwx 1 root root 13 Oct 18 15:14 nvme-
eui.0000320f5cad32cf00a0980000af4112 -> ../../nvme0n1
```

I/O run to `/dev/disk/by-id/nvme-eui.[uuid#]` will be passed directly through `/dev/nvme[subsys#]n[id#]` which has all paths virtualized underneath it using the Native NVMe multipathing solution.

You can view your paths by running:

```
# nvme list-subsys
```

Example output:

```
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000a522500000000589aa8a6
\
+- nvme0 rdma traddr=192.4.21.131 trsvcid=4420 live
+- nvme1 rdma traddr=192.4.22.141 trsvcid=4420 live
```

If you specify a namespace device when using the `nvme list-subsys` command, it provides additional information about the paths to that namespace:

```
# nvme list-subsys /dev/nvme0n1
nvme-subsys0 - NQN=nqn.1992-
08.com.netapp:5700.600a098000af44620000000058d5dd96
\
 +- nvme0 rdma traddr=192.168.130.101 trsvcid=4420 live non-optimized
 +- nvme1 rdma traddr=192.168.131.101 trsvcid=4420 live non-optimized
 +- nvme2 rdma traddr=192.168.130.102 trsvcid=4420 live optimized
 +- nvme3 rdma traddr=192.168.131.102 trsvcid=4420 live optimized
```

There are also hooks into the multipath commands to allow you to view your path information for native failover through them as well:

```
#multipath -ll
```

To view the path information, the following must be set in `/etc/multipath.conf`:

```
defaults {
        enable_foreign nvme
}
```

Example output:

```
eui.0000a0335c05d57a00a0980000a5229d [nvme]:nvme0n9 NVMe,Netapp E-
Series,08520001
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized    live
`-+- policy='n/a' prio-10 status=non-optimized
`- 0:1:1 nvme0c1n1 0:0 n/a non-optimized    live
```

Create filesystems (RHEL 7 and SLES 12)

For RHEL 7 and SLES 12, you create a file system on the desired dm device and mount the filesystem.

Steps

1. Run the `multipath -ll` command to get a list of `/dev/mapper/dm` devices.

   ```
   # multipath -ll
   ```

   The result of this command shows two devices, `dm-19` and `dm-16`:

   ```
   eui.00001ffe5a94ff8500a0980000af4444 dm-19 NVME,NetApp E-Series
   size=10G features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='service-time 0' prio=50 status=active
   | |- #:#:#:# nvme0n19 259:19  active ready running
   | `- #:#:#:# nvme1n19 259:115 active ready running
   `-+- policy='service-time 0' prio=10 status=enabled
     |- #:#:#:# nvme2n19 259:51  active ready running
     `- #:#:#:# nvme3n19 259:83  active ready running
   eui.00001fd25a94fef000a0980000af4444 dm-16 NVME,NetApp E-Series
   size=16G features='1 queue_if_no_path' hwhandler='0' wp=rw
   |-+- policy='service-time 0' prio=50 status=active
   | |- #:#:#:# nvme0n16 259:16  active ready running
   | `- #:#:#:# nvme1n16 259:112 active ready running
   `-+- policy='service-time 0' prio=10 status=enabled
     |- #:#:#:# nvme2n16 259:48  active ready running
     `- #:#:#:# nvme3n16 259:80  active ready running
   ```

2. Create a file system on the partition for each `/dev/mapper/eui-` device.

   The method for creating a file system varies depending on the file system chosen. This example shows creating an `ext4` file system.

```
# mkfs.ext4 /dev/mapper/dm-19
mke2fs 1.42.11 (09-Jul-2014)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/mapper/eui.00001ffe5a94ff8500a0980000af4444 /mnt/ext4
```

Create filesystems (RHEL 8, RHEL 9, SLES 15)

For RHEL 8, RHEL 9, and SLES 15, you create a filesystem on the native nvme device and mount the filesystem.

Steps

1. Run the multipath -ll command to get a list of nvme devices.

```
# multipath -ll
```

The result of this command can be used to find the devices associated `/dev/disk/by-id/nvme-eui.[uuid#]` location. For the example below this would be `/dev/disc/by-id/nvme-eui.000082dd5c05d39300a0980000a52225`.

```
eui.000082dd5c05d39300a0980000a52225 [nvme]:nvme0n6 NVMe,NetApp E-
Series,08520000
size=4194304 features='n/a' hwhandler='ANA' wp=rw
|-+- policy='n/a' prio=50 status=optimized
| `- 0:0:1 nvme0c0n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=50 status=optimized
| `- 0:1:1 nvme0c1n1 0:0 n/a optimized     live
|-+- policy='n/a' prio=10 status=non-optimized
| `- 0:2:1 nvme0c2n1 0:0 n/a non-optimized live
`-+- policy='n/a' prio=10 status=non-optimized
  `- 0:3:1 nvme0c3n1 0:0 n/a non-optimized live
```

2. Create a file system on the partition for the desired nvme device using the location `/dev/disk/by-id/nvme-eui.[id#]`.

   The method for creating a file system varies depending on the file system chosen. This example shows creating an ext4 file system.

```
# mkfs.ext4 /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
mke2fs 1.42.11 (22-Oct-2019)
Creating filesystem with 2620928 4k blocks and 655360 inodes
Filesystem UUID: 97f987e9-47b8-47f7-b434-bf3ebbe826d0
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

3. Create a folder to mount the new device.

```
# mkdir /mnt/ext4
```

4. Mount the device.

```
# mount /dev/disk/by-id/nvme-eui.000082dd5c05d39300a0980000a52225
/mnt/ext4
```

Verify storage access on the host

Before using the namespace, you verify that the host can write data to the namespace

and read it back.

What you'll need

An initialized namespace that is formatted with a file system.

Steps

1. On the host, copy one or more files to the mount point of the disk.
2. Copy the files back to a different folder on the original disk.
3. Run the diff command to compare the copied files to the originals.

After you finish

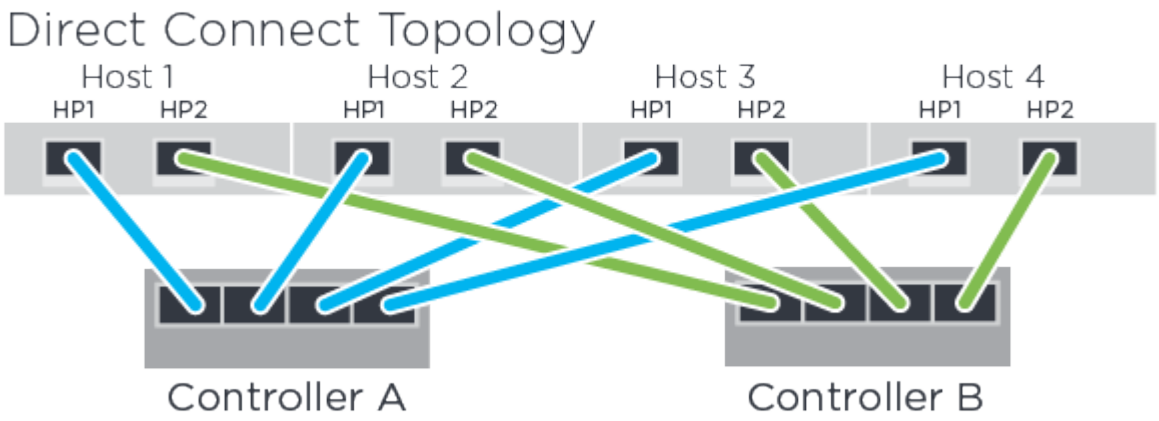
Remove the file and folder that you copied.

Record your NVMe over FC 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.

Direct connect topology

In a direct connect topology, one or more hosts are directly connected to the controller.

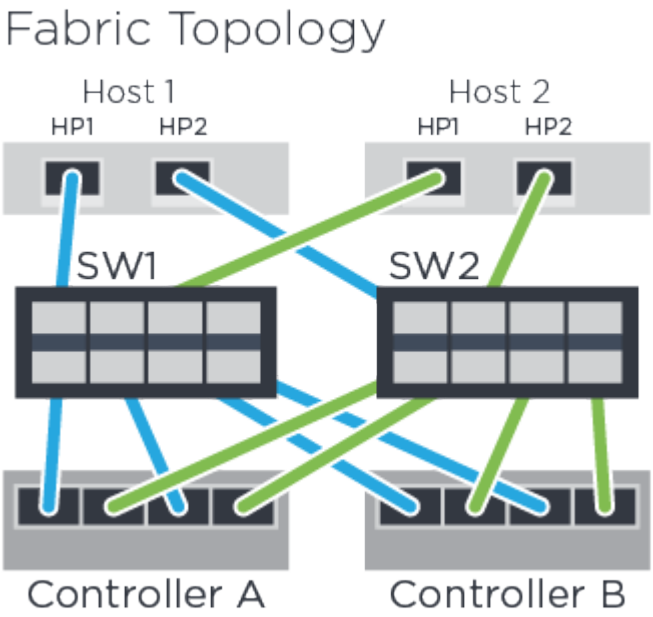


- Host 1 HBA Port 1 and Controller A Host port 1
- Host 1 HBA Port 2 and Controller B Host port 1
- Host 2 HBA Port 1 and Controller A Host port 2
- Host 2 HBA Port 2 and Controller B Host port 2
- Host 3 HBA Port 1 and Controller A Host port 3
- Host 3 HBA Port 2 and Controller B Host port 3
- Host 4 HBA Port 1 and Controller A Host port 4
- Host 4 HBA Port 2 and Controller B Host port 4

Switch connect topology

In a fabric topology, one or more switches are used. See the NetApp Interoperability Matrix Tool for a list of

supported switches.



Host identifiers

Locate and document the initiator NQN from each host.

Host port connections	Host NQN
Host (initiator) 1	
Host (initiator) 2	

Target NQN

Document the target NQN for the storage array.

Array name	Target NQN
Array controller (target)	

Target NQNs

Document the NQNs to be used by the array ports.

Array controller (target) port connections	NQN
Controller A, port 1	
Controller B, port 1	

Array controller (target) port connections	NQN
Controller A, port 2	
Controller B, port 2	

Mapping host name

The mapping host name is created during the workflow.

Mapping host name	
Host OS type	

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:

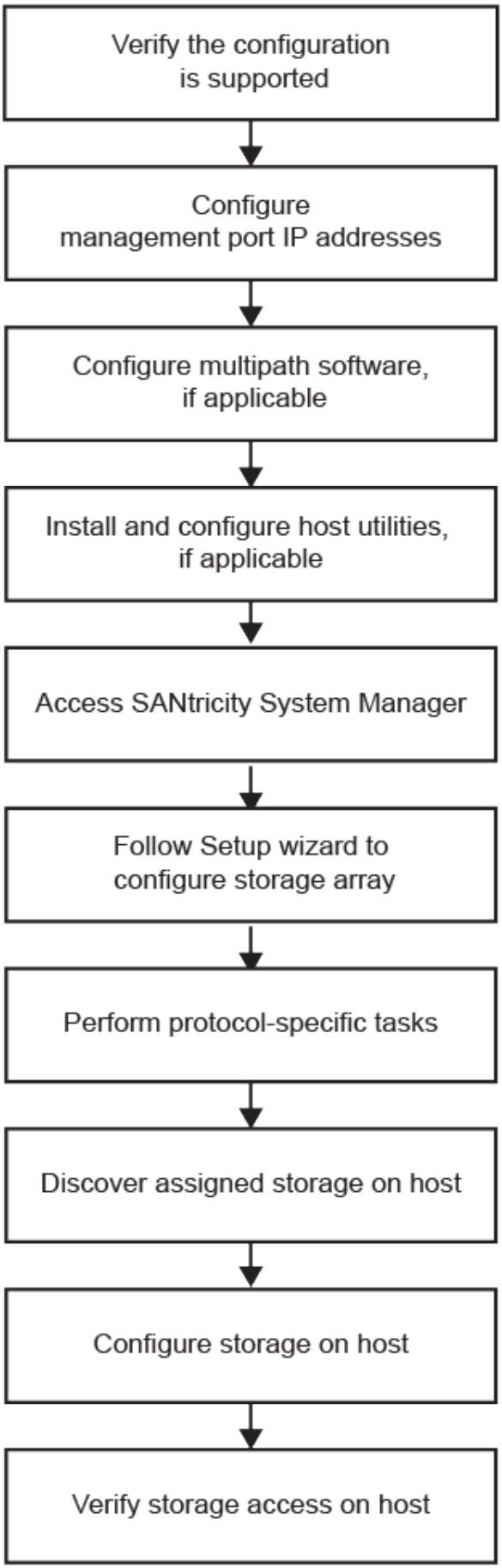
Component	Assumptions
Hardware	• You have used the Installation and Setup Instructions included with the controller shelves to install the hardware. • You have connected cables between the optional drive shelves and the controllers. • You have applied power to the storage system. • You have installed 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.

Component	Assumptions
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.
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
```

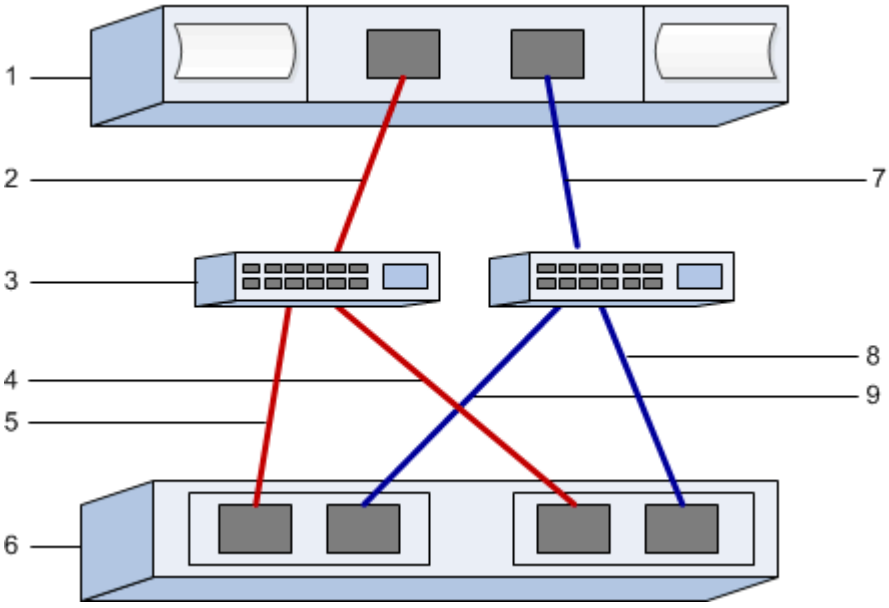
3. Record the initiator identifiers. The output will be similar to this example:

```
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**

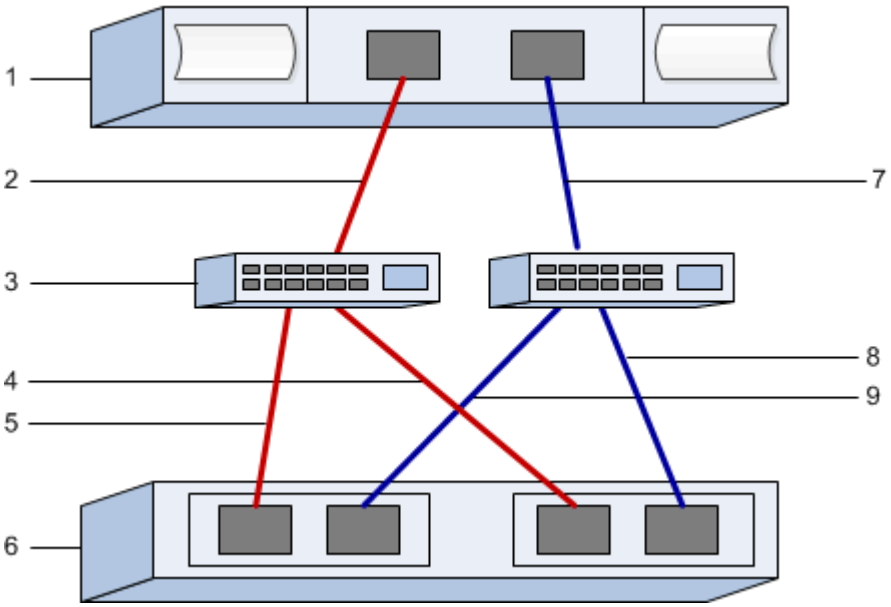
```
esxcfg-module -s "ql2xnvmesupport=1" qlnativefc
```

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*

Callout No.	Array controller (target) port connections	WWPN
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.
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.

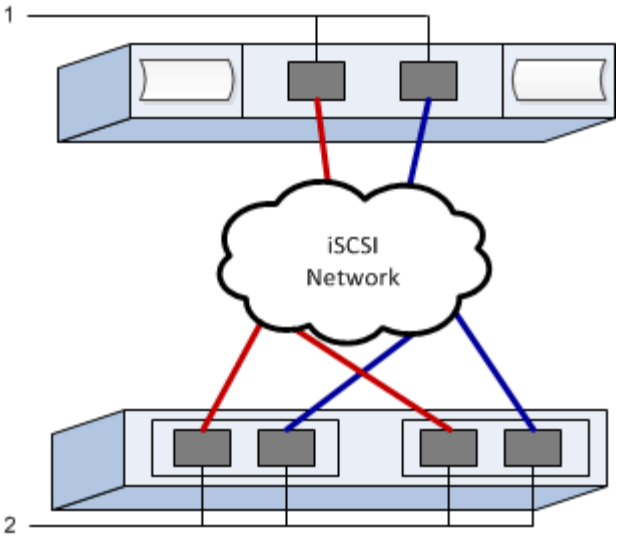
3. Return to the iSCSI Configuration procedure to finish target discovery.

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

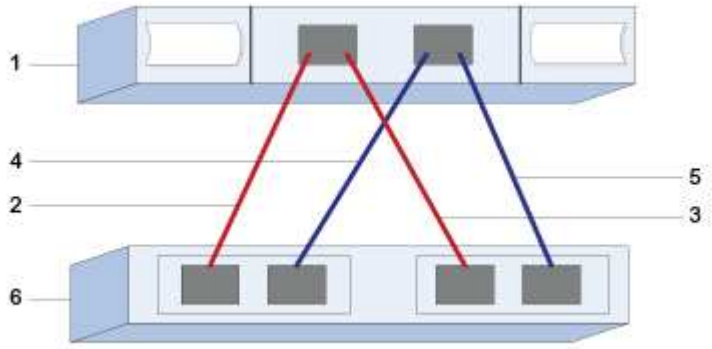
1. Download the HBA utility from your HBA vendor's web site.
2. Install the utility.

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*
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).

Windows express configuration

Windows express configuration overview

The Windows express method for installing your storage array and accessing SANtricity System Manager is appropriate for setting up a standalone Windows host to an E-Series 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 Windows workflow.

1. Set up one of the following communication environments:
   - Fibre Channel (FC)
   - 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.
- NetApp Documentation: Host Utilities — Provides documentation for the current Windows Unified Host Utilities version.

Assumptions

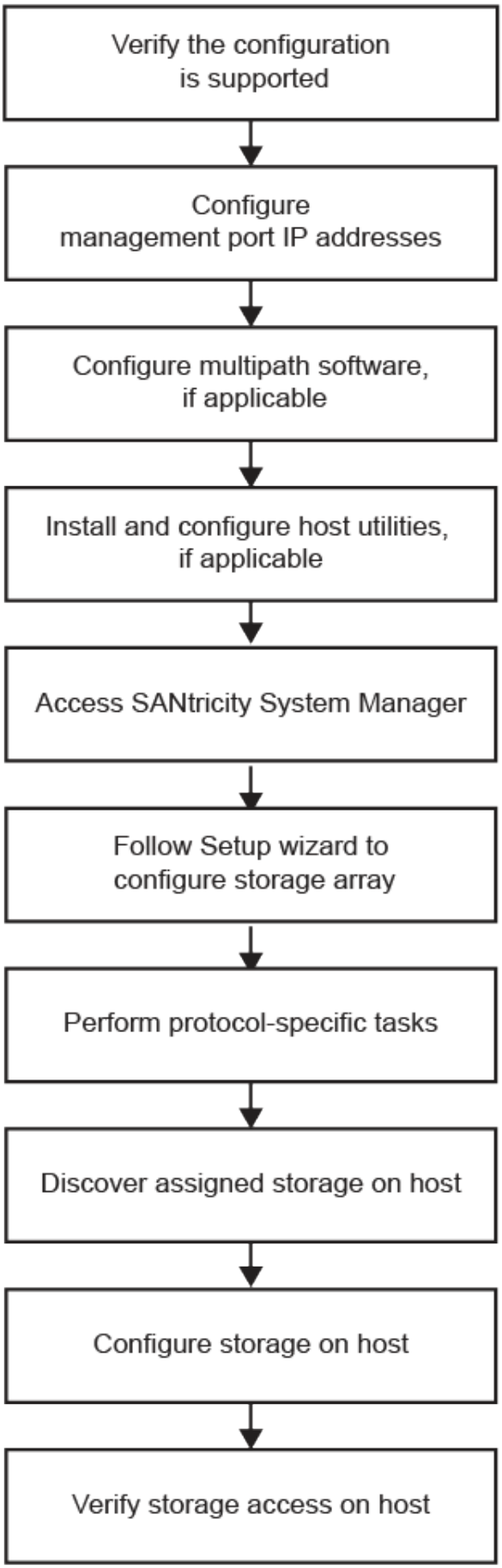
The Windows express method is based on the following assumptions:

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 Windows as a virtualized guest. • You are not configuring the data (I/O attached) host to boot from SAN.

Component	Assumptions
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.
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.

Understand the Windows workflow

This workflow guides you through the express method for configuring your storage array and SANtricity System Manager to make storage available to a Windows 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 Windows configuration is supported

To ensure reliable operation, 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 on the **Storage 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. Each HBA vendor has specific methods for updating boot code and firmware. Refer to the support section of the vendor's website to obtain the instructions and software necessary to update the HBA boot code and 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 install the SANtricity Windows DSM package and use the multipath package for Windows.

What you'll need

The correct administrator or superuser privileges.

About this task

Multipath software provides a redundant path to the storage array in case one of the physical paths is disrupted. Before you can use multipathing, you need to install the SANtricity Windows DSM package. This package contains the multipath software for Windows.

Windows installations use the native MPIO Device Specific Module (DSM) driver for failover. When you install and enable the SANtricity Windows DSM package, you do not need to take further action to use multipath.

Steps

1. Download the **SANtricity Windows DSM** package from the SANtricity OS software page. Select your software version, accept the license agreement, and select **SANtricity Windows DSM** under Additional Downloads.
2. Run the **SANtricity Windows DSM** installer. Double-click the install package to execute.
3. Use the installation wizard to install the package on the management station.

Install and configure Windows Unified Host Utilities

The Windows Unified Host Utilities tools help you to connect host computers to NetApp storage systems and set required parameters on host computers. You can also set appropriate disk timeouts for best read/write performance with NetApp storage.

For more information, see the *Windows Host Utilities Installation Guide,* found under NetApp Documentation: Host Utilities.

Steps

1. Use the NetApp Interoperability Matrix Tool to determine the appropriate version of Unified Host Utilities to install.

   The versions are listed in a column within each supported configuration.

2. Download the Unified Host Utilities from NetApp Support.

   This utilities package cannot be installed using the SANtricity Storage Manager installer.

   Alternatively, you can use the SANtricity SMdevices utility to perform the same functions as the Unified Host Utility tool. The SMdevices utility is included as part of the SMutils package. The SMutils package is a collection of utilities to verify what the host sees from the storage array. It is included as part of the SANtricity software installation.

Install SANtricity Storage Manager for SMcli and Host Context Agent (HCA)

If you are using SANtricity software 11.53 or earlier, you can install the SANtricity Storage Manager software on your management station to help manage the array.

SANtricity Storage Manager includes the command line interface (CLI) for additional management tasks, and also the Host Context Agent for pushing host configuration information to the storage array controllers through the I/O path.

If you are using SANtricity software 11.60 and newer, you do not need to follow these steps. The SANtricity Secure CLI (SMcli) is included in the SANtricity OS and downloadable through the SANtricity System Manager. For more information on how to download the SMcli through the SANtricity System Manager, refer to the *Download command line interface (CLI)* topic under the SANtricity System Manager Online Help.

What you'll need

- SANtricity software 11.53 or earlier.
- The correct administrator or superuser privileges.
- A system for the SANtricity Storage Manager client that has the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **Disk space**: 5 GB
  - **OS/Architecture**: For guidance on determining the supported operating system versions and architectures, go to NetApp Support. From the **Downloads** tab, go to **Downloads › E-Series SANtricity Storage Manager**.

Steps

1. Download the SANtricity software release at NetApp Support. From the **Downloads** tab, **Downloads › E-Series SANtricity Storage Manager**.
2. Run the SANtricity installer. Double-click the SMIA*.exe install package to execute.
3. Use the installation wizard to install the software on the management station.

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 (MSE)	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 or 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 more information, see the online help for SANtricity System Manager.

Perform FC-specific tasks

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

Step 1: Configure the FC switches—Windows

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.)

About this task

You must zone by WWPN, not by physical port. 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 host WWPNs and make recommended settings—FC, Windows

You install an FC HBA utility so you can view the worldwide port name (WWPN) of each host port. Additionally, you can use the HBA utility to change any settings recommended in the Notes column of the NetApp Interoperability Matrix Tool for the supported configuration.

About this task

Review these guidelines for HBA utilities:

- Most HBA vendors offer an HBA utility. You will need the correct version of HBA for your host operating system and CPU. Examples of FC HBA utilities include:
  - Emulex OneCommand Manager for Emulex HBAs
  - QLogic QConverge Console for QLogic HBAs
- Host I/O ports might automatically register if the host context agent is installed.

Steps

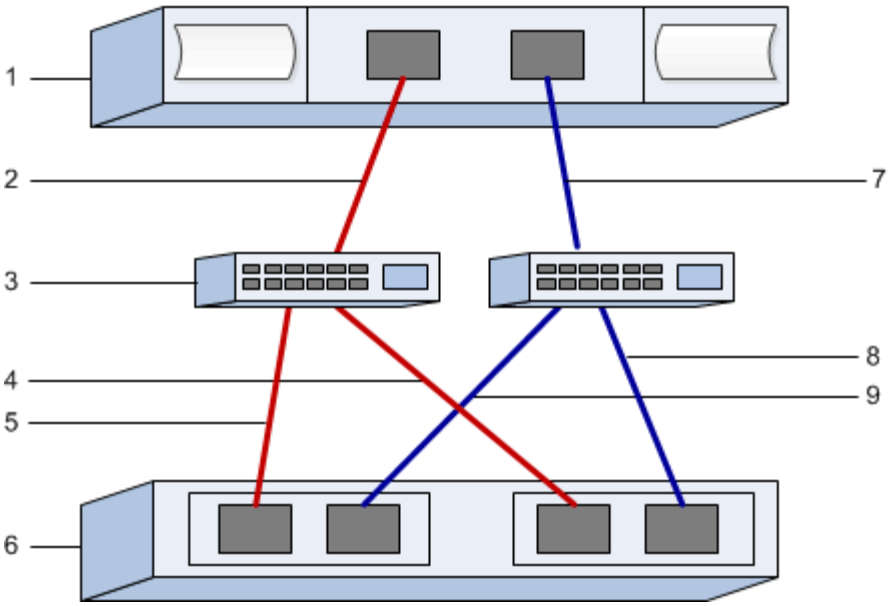
1. Download the appropriate utility from your HBA vendor's web site.
2. Install the utility.
3. Select the appropriate settings in the HBA utility.

   Appropriate settings for your configuration are listed in the Notes column of the NetApp Interoperability Matrix Tool.

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. Any single port has two paths to the storage (one to each controller).



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 name

Mapping host name	

Host OS type	

Perform iSCSI-specific tasks

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

Step 1: Configure the switches—iSCSI, Windows

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 by using VLANs or two separate networks.
- 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 Windows

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.

An effective strategy for configuring the iSCSI network with basic redundancy is to connect each host port and one port from each controller to separate switches and partition each set of host and controller ports on separate network segments using VLANs.

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 procedure in Step 3.

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, Windows

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.
- A password for the System Manager GUI, or Role-Based Access Control (RBAC) or LDAP and a directory service 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**.

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 select the **Set Password** button.

   When you open System Manager and no pools, volumes groups, workloads, or notifications have been configured, the Setup wizard launches.

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 iSCSI host interface cards in the E5700 and EF570 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.
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.
Enable VLAN support (Available by clicking **Show more settings**.)	This option is only available in an iSCSI environment. It is not available in an NVMe over RoCE environment. Select this option to enable a VLAN and enter its ID. A VLAN is a logical network that behaves like it is physically separate from other physical and virtual local area networks (LANs) supported by the same switches, the same routers, or both.
Enable ethernet priority (Available by clicking **Show more settings**.)	This option is only available in an iSCSI environment. It is not available in an NVMe over RoCE environment. Select this option to enable the parameter that determines the priority of accessing the network. Use the slider to select a priority between 1 and 7. In a shared local area network (LAN) environment, such as Ethernet, many stations might contend for access to the network. Access is on a first-come, first-served basis. Two stations might try to access the network at the same time, which causes both stations to back off and wait before trying again. This process is minimized for switched Ethernet, where only one station is connected to a switch port.

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

Step 4: Configure host-side networking—iSCSI

You must configure iSCSI networking on the host side so that the Microsoft iSCSI Initiator can establish sessions with the array.

What you'll need

- Fully configured switches that will be used to carry iSCSI storage traffic.
- Enabled send and receive hardware flow control **end to end**
- Disabled priority flow control.

- Array side iSCSI configuration completed.
- The IP address of each port on the controller.

About this task

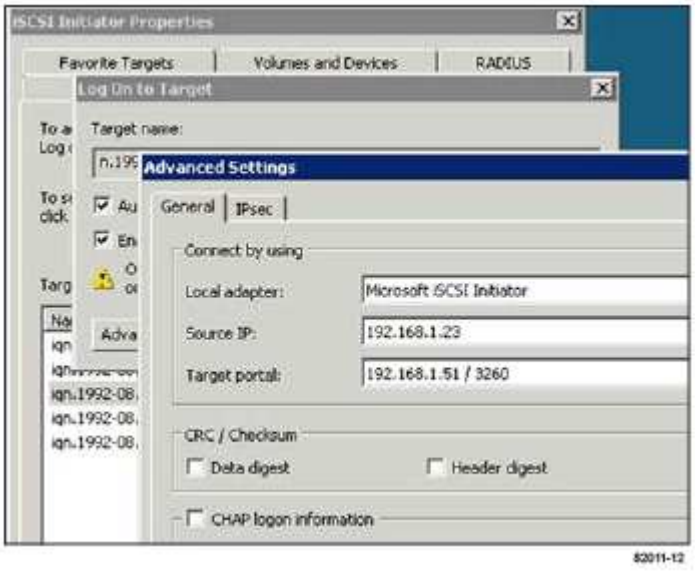
These instructions assume that two NIC ports will be used for iSCSI traffic.

Steps

1. Disable unused network adapter protocols.

   These protocols include, but are not limited to, QoS, File and Print Sharing, and NetBIOS.

2. Execute `> iscsicpl.exe` from a terminal window on the host to open the **iSCSI Initiator Properties** dialog box.
3. On the **Discovery** tab, select **Discover Portal**, and then enter the IP address of one of the iSCSI target ports.
4. On the **Targets** tab, select the first target portal you discovered and then select **Connect**.
5. Select **Enable multi-path**, select **Add this connection to the list of Favorite Targets**, and then select **Advanced**.
6. For **Local adapter**, select **Microsoft iSCSI Initiator**.
7. For **Initiator IP**, select the IP address of a port on the same subnet or VLAN as one of the iSCSI targets.
8. For **Target IP**, select the IP address of a port on the same subnet as the **Initiator IP** selected in the step above.
9. Retain the default values for the remaining check boxes, and then select **OK**.
10. Select **OK** again as you return to the **Connect to Target** dialog box.
11. Repeat this procedure for each initiator port and session (logical path) to the storage array that you want to establish.



Step 5: Verify IP network connections—iSCSI, Windows

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

1. Select **Start › All Programs › Accessories › Command Prompt**, and then use the Windows CLI to run one of the following commands, depending on whether jumbo frames are enabled:
   - If jumbo frames are not enabled, run this command:

     ```
     ping -s <hostIP\> <targetIP\>
     ```

   - 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 -f switch sets the `don't fragment (DF)` bit. The -l switch allows you to set the size. These options allow jumbo frames of 9,000 bytes to be successfully transmitted between the iSCSI initiator and the target.

     ```
     ping -l 8972 -f <iSCSI_target_IP_address\>
     ```

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

     ```
     C:\>ping -l 8972 -f 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 `ping` 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.

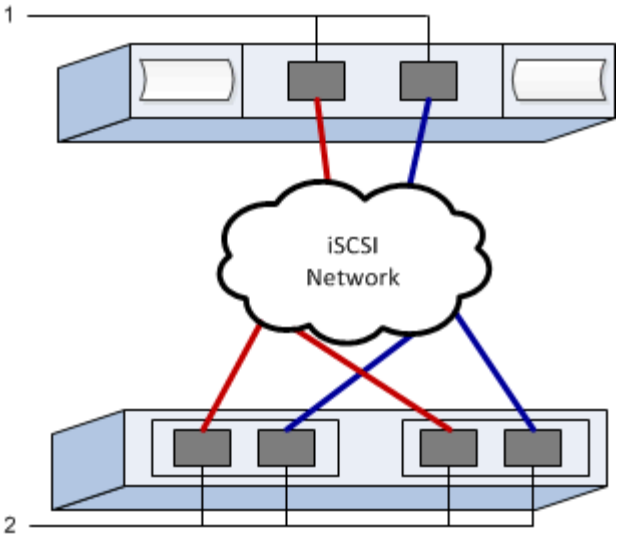
   If the command fails (for example, returns `Packet needs to be fragmented but DF set`), verify the MTU size (jumbo frame support) for the Ethernet interfaces on the host server, storage controller, and switch ports.

Step 6: Record your configuration

You can generate and print a PDF of this page, and then use the following worksheet to record iSCSI 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 appropriate settings.

Step 1: Determine SAS host identifiers—Windows

Find the SAS addresses using the HBA utility, 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. Depending on your host operating system and CPU, use either the LSI-sas2flash(6G) or sas3flash(12G) utility.
- Host I/O ports might automatically register if the host context agent is installed.

Steps

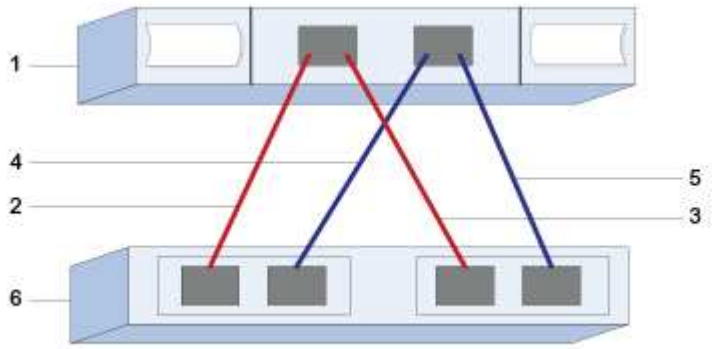
1. Download the LSI-sas2flash(6G) or sas3flash(12G) utility from your HBA vendor's web site.

2. Install the utility.
3. Use the HBA BIOS to select the appropriate settings for your configuration.

   For setting recommendations, see the Notes column of the NetApp Interoperability Matrix Tool.

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*
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

When you add new LUNs, you must manually rescan the associated disks to discover them. The host does not automatically discover new LUNs.

LUNs on your storage system appear as disks to the Windows host.

Steps

1. Log on as an administrator.
2. To discover the storage, run the following command from a Windows command prompt.

```
# echo rescan | diskpart
```

3. To verify the addition of new storage, run the following command.

```
# echo list disk | diskpart
```

Configure storage on the host

Because a new LUN is offline and has no partition or file system when a Windows host first discovers it, you must bring the volume online and initialize it in Windows. Optionally, you can format the LUN with a file system.

You can initialize the disk as a basic disk with a GPT or MBR partition table. Typically, you format the LUN with a file system such as New Technology File System (NTFS).

What you'll need

A LUN discovered by the host.

Steps

1. From a Windows command prompt, enter the `diskpart` context.

```
> diskpart
```

2. View the list of available disks.

```
> list disk
```

3. Select the disk to bring online.

```
> select disk 1
```

4. Bring the disk online.

```
> online disk
```

5. Create a partition.

```
> create partition primary
```

> In Windows Server 2008 and later, you are prompted immediately after creating the partition to format the disk and give it a name. Select **Cancel** on the prompt to continue using these instructions for formatting and naming the partition.

6. Assign a drive letter.

```
> assign letter=f
```

7. Format the disk.

```
> format FS=NTFS LABEL="New Volume" QUICK
```

8. Exit the diskpart context.

```
> exit
```

Verify storage access on the host

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

What you'll need

You must have initialized the LUN and formatted it with a file system.

Steps

1. Create and write to a file on the new LUN.

```
> echo test file > f:\\test.txt
```

2. Read the file and verify data was written.

```
> type f:\\test.txt
```

3. To verify that multipath is working, change the volume ownership.
   a. From the SANtricity System Manager GUI, go to **Storage** > **Volumes**, and then select **More** > **Change ownership**.
   b. On the Change Volume Ownership dialog box, use the **Preferred Owner** pull-down to select the other controller for one of the volumes in the list, and then confirm the operation.
   c. Verify that you can still access the files on the LUN.

```
> dir f:\\
```

4. Find the target ID.

The dsmUtil utility is case sensitive.

```
> C:\\Program Files \(x86\)\\DSMDrivers\\mppdsm\\dsmUtil.exe -a
```

5. View the paths to the LUN and verify that you have the expected number of paths. In the `<target ID>` portion of the command, use the target ID that you found in the previous step.

```
> C:\\Program Files \(x86\)\\DSMDrivers\\mppdsm\\dsmUtil.exe -g <target
ID\>
```

Copyright information

Copyright © 2022 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.