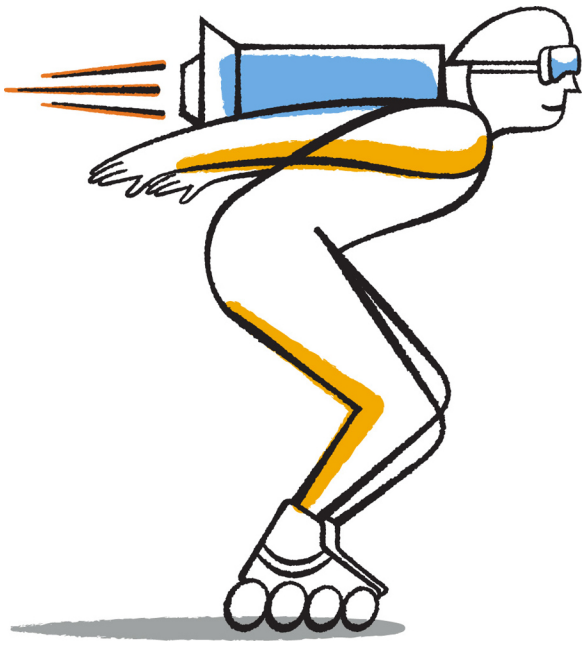
SANtricity® Storage Manager 11.20

FC Configuration and Provisioning for VMware

Express Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-09017-B0
April 2015

Contents

Deciding whether to use this guide 4
Configuration and provisioning workflow 5
Verifying that the configuration is supported 6
Related information 6
Filling out the worksheet 7
Installing and configuring SANtricity Storage Manager 9
Configuring the multipath software 14
Determining the initiator WWPNs 16
Zoning the switches 17
Deciding whether to use a disk pool or a volume group 18
Creating a disk pool 19
Creating a volume group 21
Creating a volume 22
Creating a volume from a disk pool 24
Creating a volume from a volume group 24
Defining a host in SANtricity Storage Manager 25
Mapping a volume to a host 27
Discovering mapped storage on the host 29
Configuring storage on the host 30
Verifying storage access on the host 31
If the volume has been used as a VMFS datastore 31
If the volume has been assigned to a VM as an RDM 31
Where to find additional information 32
Copyright information 33
Trademark information 34
How to send comments about documentation and receive update notifications 35

Deciding whether to use this guide

This guide describes how to install the SANtricity® Storage Manager software and how to quickly set up the FC environment, provision a LUN, and make the LUN available using an FC HBA on a VMware ESXi host. You should use this guide for setting up a standalone VMware ESXi host to E-Series or EF-Series storage systems.

This guide does not provide information about all the available options or a lot of conceptual background for the tasks.

This guide is based on the following assumptions:

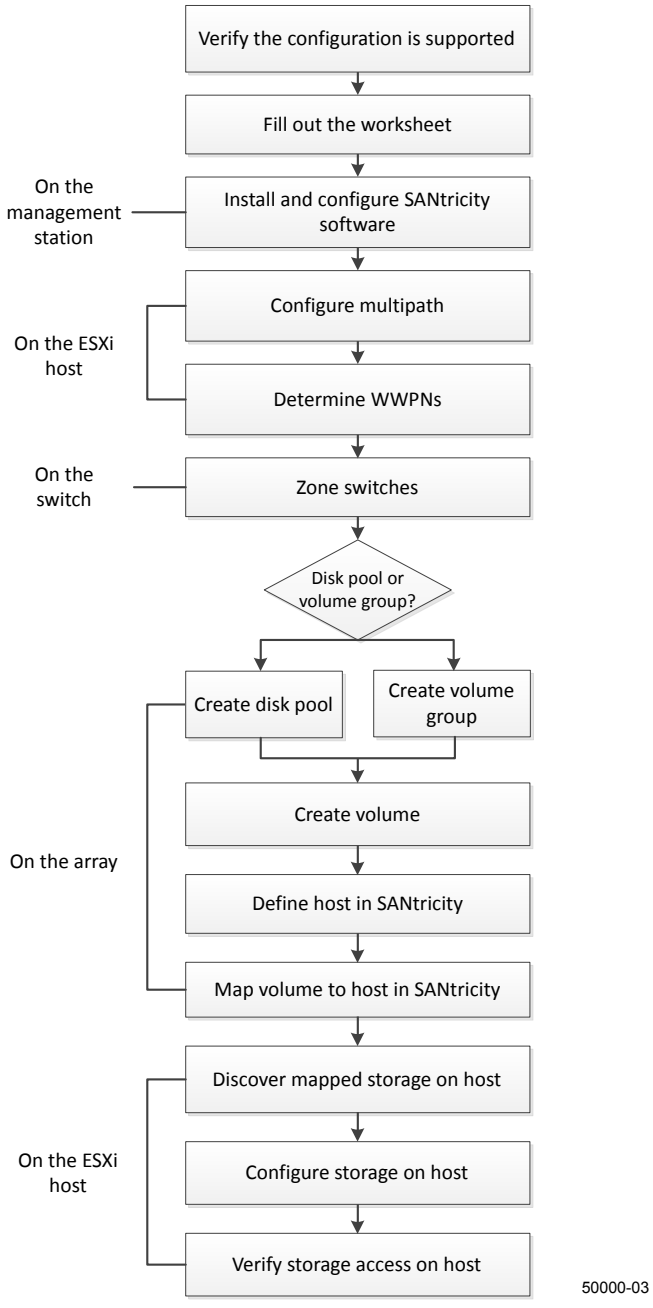
- Your storage array hardware has been successfully installed.
- All host-side Fibre Channel connections are in place, and switch zoning has been activated.
- You are using out-of-band management.
- You are using traditional FC HBAs and switches.
- All other hardware and connections are in place.
- At least one static IP address on a 1G management network has been reserved for each controller.
- You are using a management station for management rather than the data (I/O attached) host.
- During SANtricity configuration, the management station is attached to the same subnet as the storage management ports.
- You are using FC HBAs driver versions as listed on the NetApp Interoperability Matrix Tool (IMT).
- You are not configuring the data (I/O attached) host to boot from SAN.
- ESXi host is not being used as a virtualized guest.
- You are not using shared volumes.
- Host operating system is installed.
- A vCenter Server or vCenter Appliance is installed and the ESXi host has been added to its inventory OR the ESXi host is being managed directly by the vSphere Client.

If these assumptions are not correct for your installation, or if you want more conceptual background information, see the following documentation available on the NetApp Support site: *http://mysupport.netapp.com*.

- *Software Installation Reference for SANtricity Storage Manager 11.20*
- *Multipath Drivers Guide for SANtricity Storage Manager 11.20*
- *SANtricity Online Help*
- *NetApp E-Series Plug-in for VMware vCenter User Guide*

Configuration and provisioning workflow

When you make storage available to a host using FC, you provision a volume in SANtricity Storage Manager, and then map the volume to a host or host group.



Verifying that the configuration is supported

About this task

To ensure reliable operation, you must create an implementation plan and then verify that the entire configuration is supported. The *Interoperability Matrix* lists the supported configurations. This configuration includes host-O/S version, platform, feature, file system, multipath, and HBA driver requirements, supported controller and controller firmware requirements, and protocol, software initiator and storage attachment requirements.

Steps

1. Go to the *Interoperability Matrix* to verify that you have a supported combination of the following components:
   - Host computer CPU architecture (for standard rack servers)
   - Specific processor blade model (for blade servers)
   - Storage protocol
   - VMware ESXi operating system version
   - Host Bus Adapter (HBA) component
2. Select the desired components in the Component Explorer, and then select **Add Components**. Select the **Show Results** button and select the configuration in the **Name** column. Details for that configuration are displayed in the **Configuration Details** window.
3. Review the information in the following tabs in the **Configuration Details** window:
   - **Notes**: Lists important alerts and notes that are specific to your configuration. Review the alerts to identify the hotfixes that are required for your operating system.
   - **Policies and Guidelines**: Provides general guidelines for all SAN configurations.
4. Make necessary updates:
   - Update HBA driver, firmware, and bootcode as necessary.
   - You might need to install out-of-box drivers to ensure proper functionality and supportability. You can easily 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 KB article at *http://kb.vmware.com* regarding using the ESXi shell in ESXi 5.x. For installation commands, refer to the instructions that accompany the HBA drivers .
   - You might need to update the HBA bootcode and firmware to ensure proper functionality and supportability. Each HBA vendor has specific methods for updating bootcode and firmware. Some of these methods could include the use of a vCenter plugin or the installation of CIM provider on the ESXi host. Refer to the support section of the vendor's website to obtain the instructions and software necessary to update the HBA bootcode and/or firmware. Refer to the *VMware Compatibility Guide* or the HBA vendor's website to obtain the correct bootcode and/or firmware.

Related information

Interoperability Matrix: *http://mysupport.netapp.com/matrix*

Filling out the worksheet

As you progress through the sections in this guide, fill out the worksheet. You require initiator identifiers, target identifiers, and storage configuration information to perform provisioning tasks.

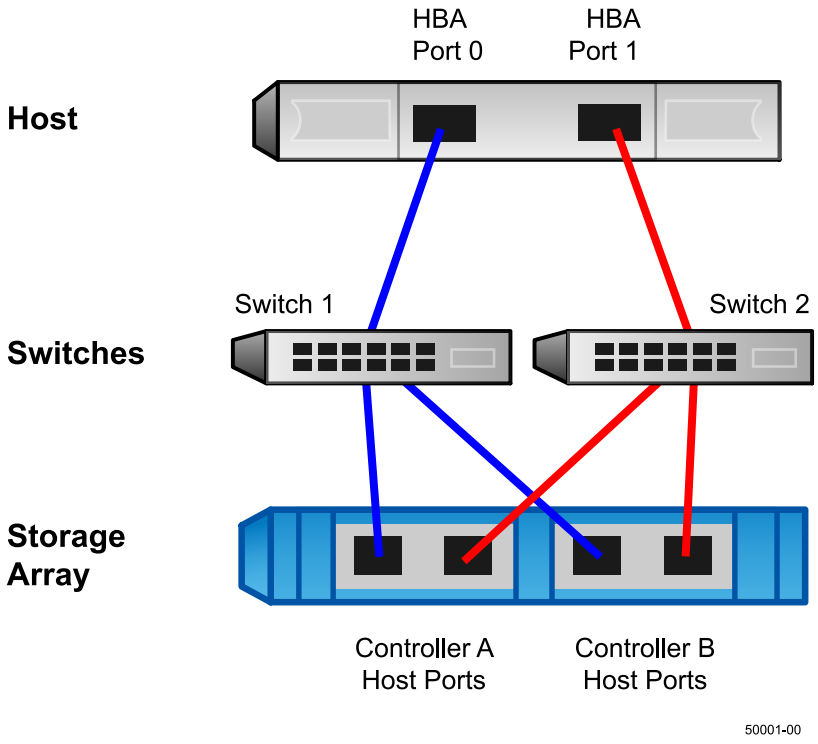
Host Identifiers

Note: The initiator WWPNs are determined during the workflow, in the “Determining the initiator WWPNs” task.

Port	WWPN
Initiator (host) port connected to FC switch 1	
Initiator (host) port connected to FC switch 2	

Target Identifiers

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



Target	WWPN
Target (storage) port controller A connected to FC switch 1	
Target (storage) port controller B connected to FC switch 1	
Target (storage) port controller A connected to FC switch 2	

Target	**WWPN**
Target (storage) port controller B connected to FC switch 2	

Mapping Host

Note: The mapping host name is created during the workflow, in the “Defining a host in SANtricity Storage Manager” topic.

Mapping Host Name	
Host OS Type	

Installing and configuring SANtricity Storage Manager

You can install the SANtricity software on a variety of operating systems to manage your storage. A graphical user interface (GUI) as well as a command line interface (CLI) are installed by default. These instructions assume you will install SANtricity Storage Manager GUI on a management station and *not* on the I/O host.

Before you begin

- Make sure you have the correct administrator or superuser privileges to install the software.
- Make sure you have followed the instructions in the *Installation and Setup Instructions* to configure your network to use a private network with the default IP addresses. The *Installation and Setup Instructions* explains how to do the physical connections and how to initialize the controller management ports to use the default IP addresses. In this procedure, you will finish setting up the private network and then configure the permanent, static IP addresses of the controller management ports.
- Make sure the system that will contain the SANtricity Storage Manager client has the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **CPU speed**: Use the Interoperability Matrix Tool (*NetApp Interoperability Matrix Tool*) to confirm that your host's processor is supported. All speeds available for a supported CPU are sufficient to run the SANtricity Storage Manager.
  - **Temporary disk space**:

Operating system	Available temporary disk space (MB)
Windows Server 2008 R2	434
Windows Server 2012	434
Linux	390
Solaris	540
AIX	525

About this task

You will install the SANtricity Storage Manager software on the management station. This section describes the procedures for installing SANtricity Storage Manager on the Windows platform only. After installing SANtricity Storage Manager, you will finish configuring the private network, add the storage array to the Enterprise Management Window (EMW), name the storage array, configure the correct static IP address, subnet mask, and gateway for each controller to match the IP scheme used in the user’s network, and disable the automatic Disk Pool Creation wizard.

For more information regarding installation methods and customizations, see *Software Installation Reference Guide for SANtricity Storage Manager 11.20*.

Steps

1. Download the SANtricity software release from NetApp support site: *NetApp Support*.
2. Execute the SANtricity installer. Double-click the `SMIA*.exe` install package to execute.

3. Install the software on the management station using the installation wizard.
   a. Read the **Introduction** screen, and then select **Next**.
   b. On the **License Agreement** screen, read the agreement, select the **I accept the terms of the License Agreement** radio button, and then select **Next**.
   c. On the **Choose Install Folder** screen, select the radio button for the installation directory for the software, and then select **Next**.
   d. On the **Select Installation Type** screen, select the **Management Station** radio button, and then select **Next**.

      Note: A management station installation is not appropriate for the data host.

   e. On the **Automatically Start Monitor** screen, select the **Automatically start monitor** radio button, and then select **Next**.

      Note: Only the primary management station should run the monitor function. When installing the SANtricity software on laptops or secondary management stations, select **Do not automatically start the monitor**.

   f. On the **Pre-Installation Summary** screen, review the information, and then select **Install**.
   g. On the **Install Complete** screen, select **Done**.
4. Change the IP address on the TCP/IP port on the management station so that it will reside on the same private network as the controllers.
   a. If you have a static IP address, make note of the current IP address of the management station so that you can revert back to it after you have completed the procedure.
   b. Change the IP address. Refer to your operating system documentation for instructions on how to change the network settings on the management station and how to verify that the address has changed.

      Note: You must set the IP address for the management station to something other than the controller IP addresses (for example, use 192.168.128.100 for an IPv4 network, or use FE80:0000:0000:0000:02A0:B8FF:FE29:1D7C for an IPv6 network.

      Note: In an IPv4 network, the default IP addresses for Ethernet port 1 on controller A and controller B are 192.168.128.101 and 192.168.128.102, respectively.

   c. If your network is an IPv4 network, check the subnet mask to verify that it is set to 255.255.255.0, which is the default setting.
   d. From a command prompt, ping each of the controller IPs to make sure they are accessible.

      Example

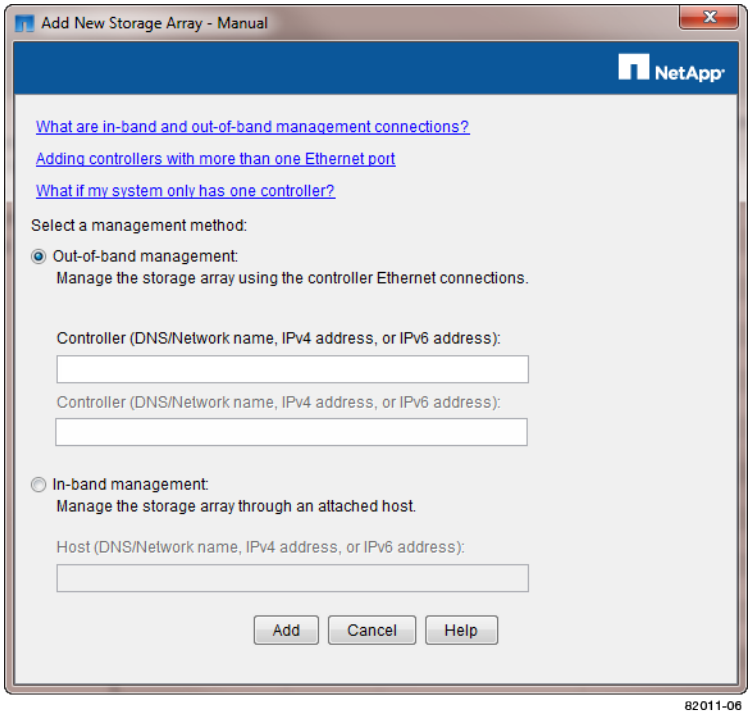
```
> ping 192.168.128.101
Reply from 192.168.128.101: bytes = 32 time<1ms TTL = 64
Ping statistics for 192.168.128.101:
Packets: Sent = 4, Received =4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms
```

```
> ping 192.168.128.102
Reply from 192.168.128.102: bytes = 32 time<1ms TTL = 64
Ping statistics for 192.168.128.102:
Packets: Sent = 4, Received =4, Lost = 0 (0% loss)
```

```
Approximate round trip times in milli-seconds:
Minimum = 0 ms, Maximum = 0 ms, Average = 0 ms
```

5. Open the **SANtricity Storage Manager** from the Windows **Start** menu. The **Enterprise Management Window (EMW)** is displayed.
6. On the **Select Addition Method** screen, select the **Manual** radio button, and then select **OK**.
7. To add one or more new storage arrays, complete the following steps:
   a. On the **Add New Storage Array – Manual** screen, make sure that the default **Out-of-band management** radio button is selected. Enter the IP address assigned to controller A, port 1, and controller B, port 1, on the storage array you are adding. You used the *Installation and Setup Instructions* to configure the default addresses. The default addresses are:

```
Controller A (port 1): IP Address : 192.168.128.101
Controller B (port 1): IP Address : 192.168.128.102
```

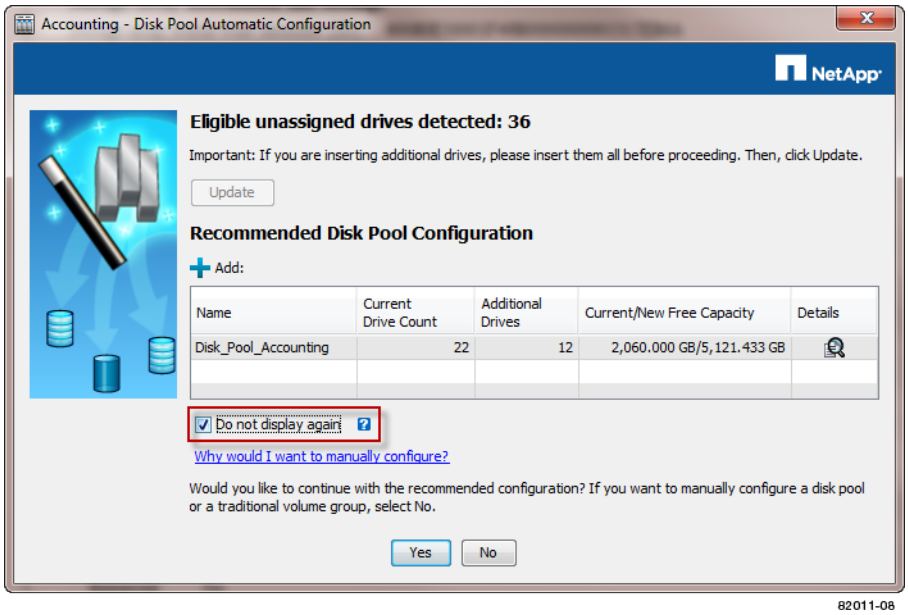


   b. Select **Add**. The **Storage Array Added** screen is displayed.
   c. On the **Storage Array Added** screen, select **Yes** to add more storage arrays, otherwise select **No**.
   d. In the **Enterprise Management Window (EMW) Devices** tab, double-click the storage array to open the **Array Management Window (AMW)**.

      Note: When you open the **AMW** for a storage array for the first time, the **Disk Pool Automatic Configuration** wizard is displayed. This wizard can be used to provision a new storage array so that a single disk pool uses all of the available capacity that meets the criteria for a disk pool. Because the automatic wizard does not offer all of the features available with disk pools, NetApp recommends creating disk pools using a different procedure, described in *Creating a disk pool* on page 19.

8. Turn off the **Disk Pool Automatic Configuration** wizard using the following steps:

a. On the **Disk Pool Automatic Configuration** dialog box, select the **Do Not Display Again** checkbox.



b. Select the **No** button to permanently dismiss the automatic configuration wizard.

9. Name the storage array so you can find it more easily in the **EMW** after you change the IP addresses:

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

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

c. In the **Storage array name** field, type a name for the storage array.

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

d. Select **OK**.

e. On the **Name/Rename Storage Arrays** warning dialog, select **Yes** to dismiss the warning and continue.

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

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

b. Select the visual representation of one of the controllers in the **Hardware** tab.

c. Right-click, then select **Controller > Configure > Management Ports**.

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

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

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

g. Depending on the format you have selected, enter the network configuration information (IP address, subnet mask, and gateway or IP address and routable IP address) in the **IPv4 Settings** tab or the **IPv6 Settings** tab.

   Note: You must obtain the network configuration information from your network administrator.

h. Select Controller B, Port 1 in the **Ethernet Port** drop down list, and repeat Step ***10.e*** through Step ***10.g*** for controller B.

i. Select **OK**.

j. Close the **AMW**.

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

12. Disconnect the private network you set up using the *Installation and Setup Instructions* and reconnect into your regular LAN.

a. Disconnect the management station from the switch or hub and reconnect it into your LAN.

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

c. Disconnect port 1 of each controller from the switch or hub and reconnect it into your LAN.

13. Add the storage array back to the **EMW** by completing the following steps:

a. Select the **Edit > Add Storage Array**option in the **EMW**.

b. On the **Add New Storage Array-Manual** screen, make sure that the default **Out-of-band management** radio button is selected.

c. Enter the IP addresses assigned to controller A, port 1, and controller B, port 1. Use the addresses you added in Step *10*.

d. Press the **Add** button.

e. On the **Storage Array Added** screen select **Yes** to add more storage arrays, otherwise select **No**.

14. Find the WWPNs of the controller host ports.

a. From the **AMW Monitor** menu, select **Reports > Storage Array Profile**.

b. Select the **Controllers** tab. Scroll through the information to find the WWPNs.

c. Record the WWPNs in the worksheet.

Configuring the multipath software

Multipathing with VMware ESXi is handled natively by NMP. NMP uses various plugins that handle the specific failover implementation of different vendors' storage arrays. The NMP plugin that is used with E-Series arrays and EF-Series arrays is VMW_SATP_ALUA.

Before you begin

You must have access to the ESXi host through the ESXi shell or remotely through SSH.

NMP claim rule modifications

Any changes that might be required to the default NMP claim rules depend on both the array model and the version of the ESXi operating system in question. Note the following versions and the changes that are required.

For **E2600, E5400, and EF540** E-Series arrays, the following versions of the ESXi operating system require the indicated command to be executed:

- ESXi 5.5 (Build 1331820)
- ESXi 5.1 (All versions)
- ESXi 5.0 (All versions prior to ESXi 5.0 P12 Build 1489271)

```
esxcli storage nmp satp rule add -s VMW_SATP_ALUA -V LSI -M INF-01-00 -c
tpgs_on -o reset_on_attempted_reserve -P VMW_PSP_MRU
```

For **E2700, E5500, EF550, E5600, and EF560** E-Series arrays, the following versions of ESXi required the indicated command to be executed:

- ESXi 5.1 (All versions prior to ESXi 5.1 U2 Build 1483097)
- ESXi 5.0 (All versions prior to ESXi 5.0 U3 Build 1311175)

```
esxcli storage nmp satp rule add -s VMW_SATP_ALUA -V NETAPP -M INF-01-00
-c
tpgs_on -o reset_on_attempted_reserve -P VMW_PSP_RR
```

VAAI claim rule modifications

Any changes that might be required to the default VAAI claim rules depend on both the array model and the version of the ESXi operating system in question. Note the following versions and the changes that are required.

The changes to the default VAAI claim rules listed below are appropriate for the following E-Series arrays:

- E2700
- E5500
- EF550
- E5600
- EF560

The following versions of the ESXi operating system require the indicated commands to be executed:

- ESXi 5.1 (All versions)
- ESXi 5.0 (All versions)

```
esxcli storage core claimrule remove -r 65433 -c Filter
esxcli storage core claimrule remove -r 65433 -c VAAI
esxcli storage core claimrule add -r 65433 -t vendor -P VAAI_FILTER
-c Filter -V NETAPP -M "LUN*"
esxcli storage core claimrule add -r 65433 -t vendor -P VMW_VAAIP_NETAPP
-c VAAI -V NETAPP -M "LUN*"
```

Determining the initiator WWPNs

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
```

Zoning the switches

Zoning the FC switches enables the hosts to connect to the storage and limits the number of paths. You zone the switches using the management interface of the switches.

Before you begin

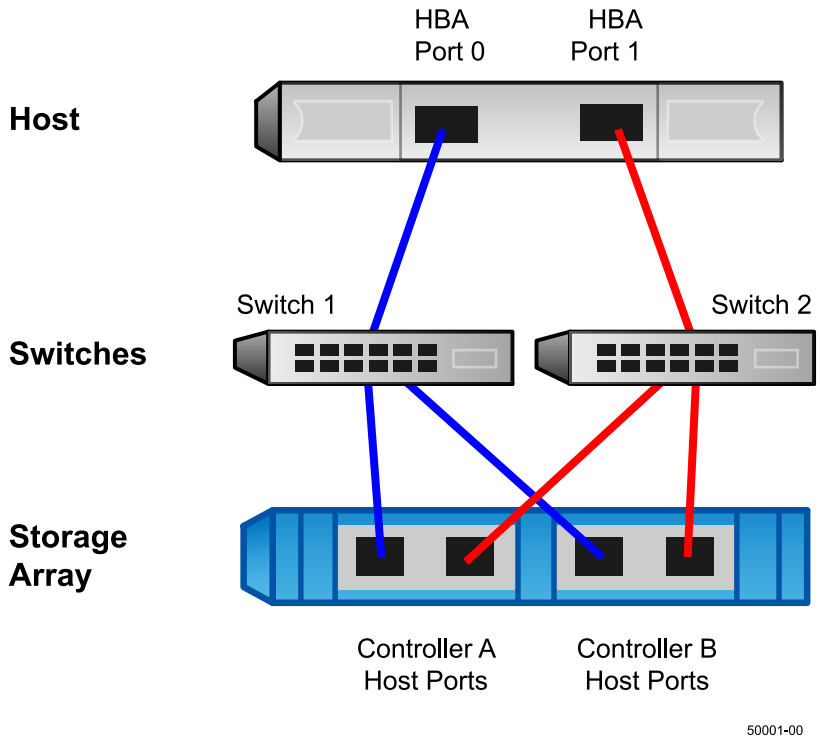
- You must have administrator credentials for the switches.
- You must know the WWPN of each host initiator port and of each controller target port connected to the switch. Use the worksheet to validate the ports.

About this task

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

You should zone by WWPN, not by physical port. Each initiator port should be in a separate zone with all of its corresponding target ports.

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



Steps

1. Log in to the FC switch administration program and select the zoning configuration option.
2. Create a new zone that includes the first initiator 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 initiator in the host.
4. Save the zones and activate the new zoning configuration.

Deciding whether to use a disk pool or a volume group

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

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

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

After you have made your decision, go to either *Creating a disk pool* on page 19 or *Creating a volume group* on page 21 to continue.

Use Case	Volume Group	Dynamic Disk Pool
Workload - Random	Good	Better
Workload - Sequential	Better	Good
Drive Rebuild Times	Slower	Faster
Performance (Optimal Mode)	Good. Best for large block, sequential workloads	Good. Best for small block, random workloads
Performance (Drive Rebuild Mode)	Degraded. Up to 40% drop in performance	Better
Multiple Drive Failure	Less data protection. Slow rebuilds, greater risk of data loss	Greater data production. Faster, prioritized rebuilds
Adding Drives	Slower. Requires Dynamic Capacity Expansion operation	Faster. Add to disk pool on the fly
Thin Provisioning support	No	Yes **Note:** No SCSI unmap support
SSDs	Yes	Yes
Simplified Administration	No. Allocate global hot spares, configure RAID	Yes. No hot spare or RAID settings to configure
Tunable Performance	Yes	No

Creating a disk pool

Using SANtricity Storage Manager, create a logical group of drives for volume creation using a disk pool.

Steps

1. From the **Array Management Window (AMW) Storage & Copy Services** tab, select **Total Unconfigured Capacity**.

   Note: If there is more than one drive type, such as SAS and SSD drives, you cannot create a disk pool from the high-level **Total Unconfigured Capacity** object. Instead, you must select a sub-object under that high-level object.

2. Right-click either the high-level object or a sub-object of **Total Unconfigured Capacity**, and then select **Create Disk Pool**.

3. From the **Create Disk Pool** dialog box, configure the attributes of the disk pool:

   a. Enter a descriptive name for the disk pool.

      Note: Disk pool names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens (-), and pound signs (#). Choose a descriptive name for the volume group to make it easier for data center administrators to manage the storage resources over time.

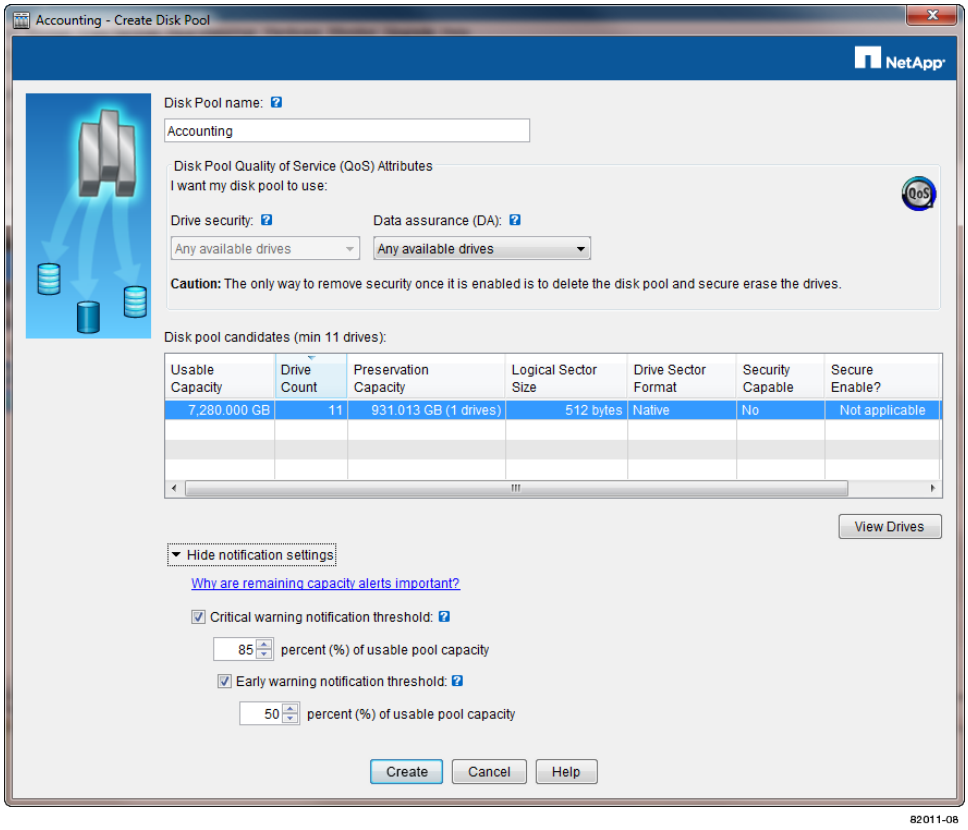
   b. Select whether you want to see any available drives, or just security capable drives. Similarly, select whether you want to see any available drives, or just data assurance (DA)-capable drives.

   c. Select the size of the disk pool from the disk pool candidates.

   d. Expand the **View Notification Settings**. Select the desired critical and early warning threshold percentages based on the specific environmental requirements for maintaining unprovisioned capacity in the disk pool.

      Note: The default percentages are 50 percent for the early warning notification threshold and 85 percent for the critical warning notification threshold. If you are intentionally provisioning most of the storage in the disk pool, for example in a big data or video application environment, consider raising the thresholds from the default levels so that the array does not enter a Needs Attention state so quickly.

      Note: Setting both thresholds to 100 percent disables the warning thresholds.



4. Select **Create**.
5. From the **Storage & Copy Services** tab, select the **Disk Pools** object in the Storage Array tree and verify the disk pool was created.
6. Go to *Creating a volume* on page 22.

Creating a volume group

Using SANtricity Storage Manager, create a logical group of drives for volume creation using a volume group.

Steps

1. Verify that hot spare coverage is adequate for the storage array.
   a. From the **Array Management Window (AMW) Hardware** menu, select **Hot Spare Coverage**.
   b. On the **Hot Spare Drive Options** dialog box, select **View/change current hot spare coverage**.
   c. On the **Hot Spare Coverage** dialog box, view coverage. If you need to select more drives for hot spares, select the **Assign** button and select hot spare drives on the **Assign Hot Spare** dialog box.

      Note: For information on how to determine if coverage is adequate, select the hyperlink "*Tips on providing hot spare coverage*" on the Hot Spare Coverage dialog box.

2. Select the **Storage & Copy Services** tab, right-click **Total Unconfigured Capacity**, and select **Create Volume Group**.

   Note: If there is more than one drive type, such as SAS and SSD drives, you cannot create a volume group from the high-level **Total Unconfigured Capacity** object. Instead, you must select a sub-object under that high-level object.

3. On the **Introduction** page of the wizard, select **Next**.
4. On the **Volume Group Name & Drive Selection** page of the wizard, perform the following steps:
   a. Enter a name for the new volume group.

      Note: Volume group names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens (-), and pound signs (#). Choose a descriptive name for the volume group to make it easier for data center administrators to manage the storage resources over time.

   b. Select the **Automatic (Recommended)** radio button from the **Drive selection choices** list, and select **Next**.
5. On the **RAID Level and Capacity** page, perform the following steps:
   a. Select the desired RAID level for the new volume group from the drop-down list.

      Note: For information on the best RAID level, select the hyperlinks "*What RAID level is best for my application?*" and "*What is tray loss protection?*" on the RAID Level and Capacity page.

   b. Select the desired volume group configuration from the list of available configurations and select **Finish**.
   c. The **volume group** wizard automatically displays a prompt for you to create a volume in the newly created volume group. To create a volume immediately, select **Yes** to continue with the volume creation. Go to *Creating a volume* on page 22.

Creating a volume

Using SANtricity Storage Manager, create volumes on a storage array for the attached host to access. You create a volume from the free capacity of either a disk pool or a volume group.

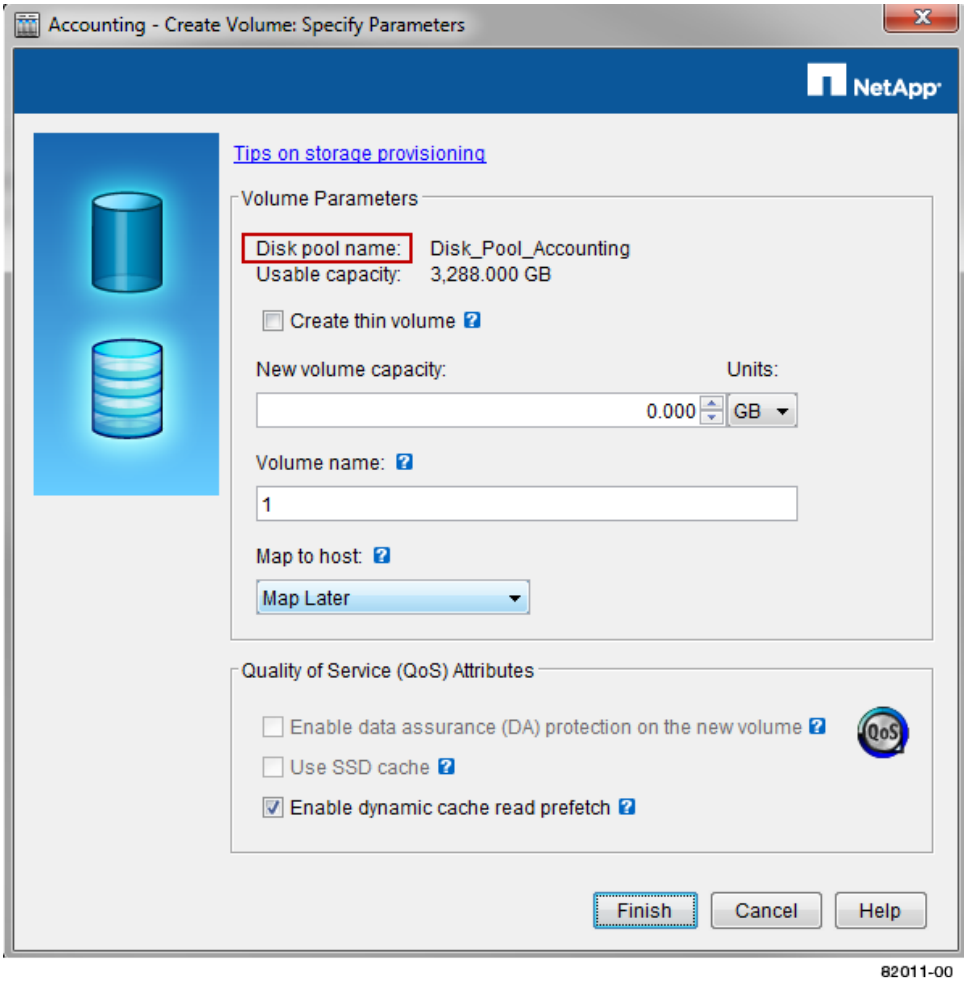
Before you begin

Determine the expected capacity, usage, data protection, and performance requirements for the volume.

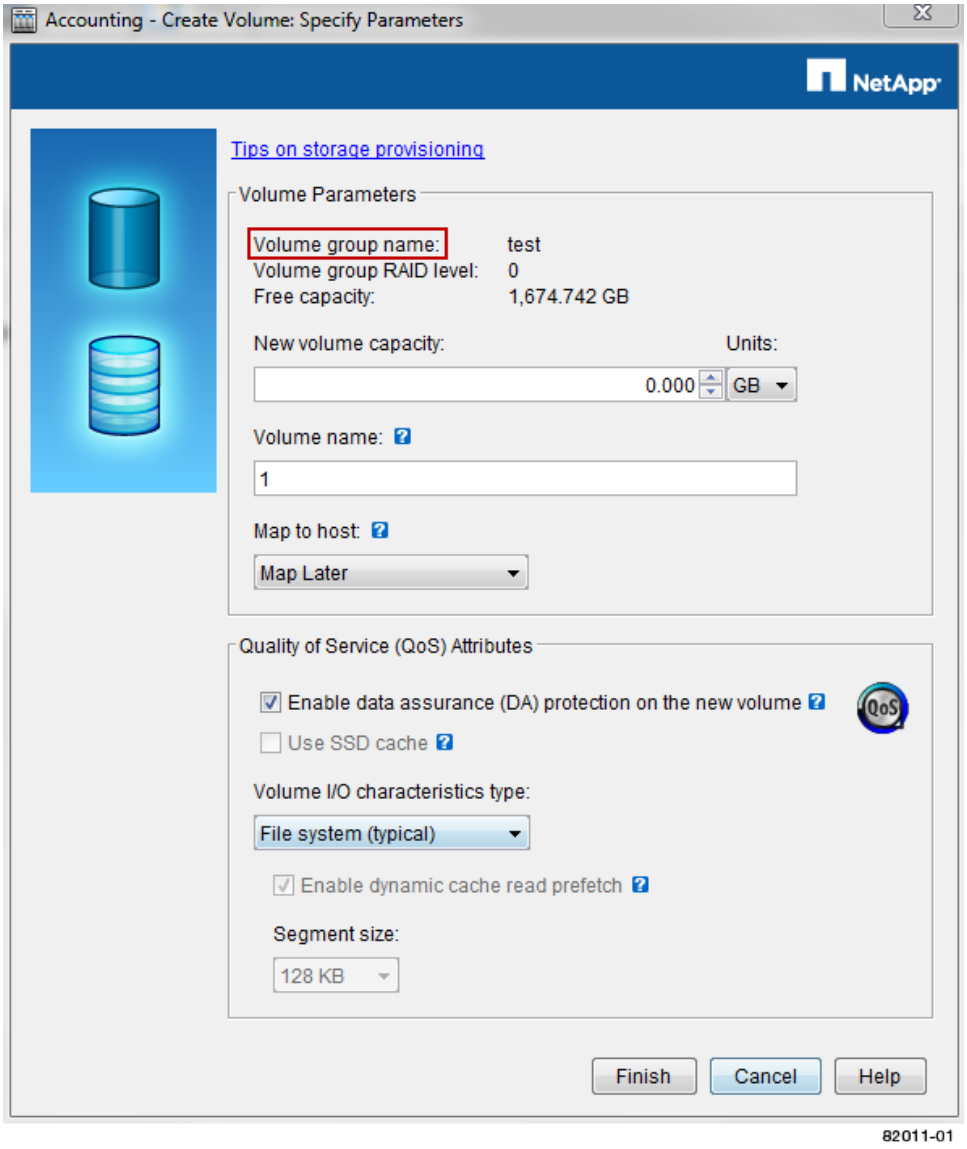
Steps

1. From the **Array Management Window (AMW) Storage & Copy Services** tab, expand the disk pool or volume group on the array where the new volume will be created.
2. Right-click **Free Capacity** > **Create Volume**.

   Note: If you are creating a volume on a disk pool, the following dialog box appears.



   Note: If you are creating a volume on a volume group, the following dialog box appears.



3. Configure the volume parameters, using the onscreen flyovers to get more information about particular options.

   a. If you are creating the volume on a disk pool and want to create a thin volume, select the **Create thin volume** checkbox.

      Note: Thin volumes cannot be created on a volume group. If you are creating the volume on a volume group, this checkbox does not appear.

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

   c. Specify the volume capacity to be taken from the free capacity that you selected in either the disk pool or the volume group.

   d. Enter the volume name.

      Note: The volume name must not exceed 30 characters and cannot contain spaces. Use underscores or dashes to separate elements within the volume name (for example, Test_Volume_1_TVG1).

   e. In the **Map to host** drop down, select the **Map later** option.

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

   Note: The **Use SSD cache** checkbox is not available in the Quality of Service section because you have chosen to map the volume to a host later. See the SANtricity online help topic "Learn about SSD Cache" to decide if it is appropriate to enable it later. To enable it, from the **AMW Storage & Copy Services** tab, right-click the volume and then select **SSD Cache > Enable**.

   a. To enable DA protection, select the **Enable data assurance (DA) protection on the new volume** checkbox.

      This option is available only if you have created the volume group or disk pool using DA-capable drives and the DA premium feature is enabled.

   b. Finish selecting the Quality of Service Attributes and create the volume. The steps vary depending on whether you are creating the volume from a disk pool or a volume group:

Creating a volume from a disk pool

About this task

This procedure is a continuation of the "Creating a volume" procedure. Before performing these steps, you must perform the steps listed in *Creating a volume* on page 22.

Steps

1. Select the **Enable dynamic cache read prefetch** checkbox to enable it.

   Note: Dynamic cache read prefetch is not available for thin volumes.

2. Select **Finish**.

Creating a volume from a volume group

About this task

This procedure is a continuation of the "Creating a volume" procedure. Before performing these steps, you must perform the steps listed in *Creating a volume* on page 22.

Steps

1. Based on the type of volume usage, select a type from the **Volume I/O characteristics type:** drop down list.

   - Selecting **File System**, **Database**, or **Multimedia** from the list automatically configures the optimal segment size and cache settings for the best performance.
   - For less common volume usages, select **Custom** from the **Volume I/O characteristics type:** list. Then, select the **Enable dynamic cache read prefetch** checkbox, if appropriate for your environment, and select the appropriate segment size from the **Segment size** list. See the *SANtricity online help* to learn more about performance tuning.

2. Select **Finish**.

Defining a host in SANtricity Storage Manager

Use SANtricity Storage Manager to allow the volumes to be shared with the host.

About this task

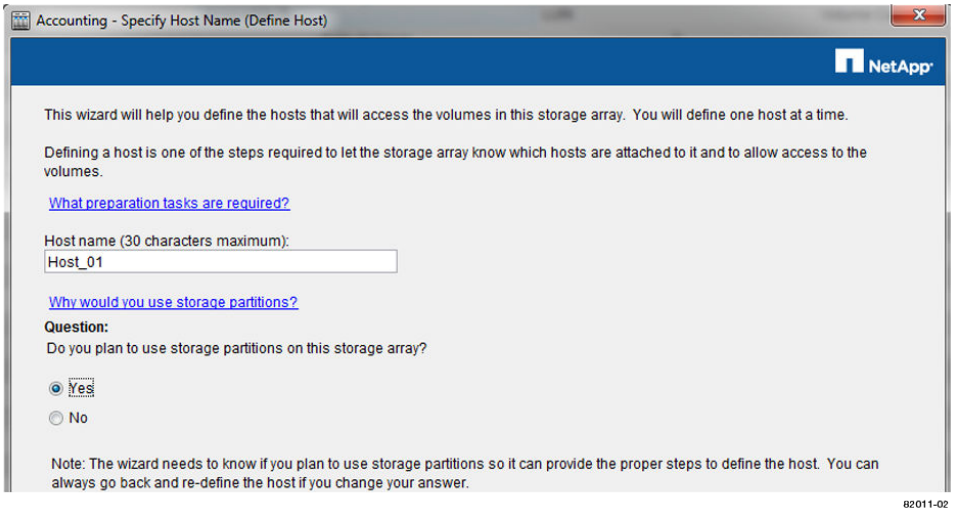
You will define a new logical host on the storage array so that volumes can be shared with the host. The recommended host type is **VMWARE**.

Steps

1. From the **Array Management Window (AMW)**, select the **Host Mappings** tab.
2. In the left pane, expand the storage array tree.
3. Right-click **Default Group** and select **Define > Host** to start the **Define Host** wizard.
   a. Enter a descriptive name for the host to make it easier for administrators to manage the environment over time.

      Note: Host names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores(_), hyphens (-), and pound signs (#).

   b. In the **Question** area of the dialog box, keep the **Yes** selected.



4. Select **Next**.
5. If you have multiple host interface types supported by the controller, you must select one from the **Choose a host interface type:** drop down.
6. Choose a method for adding a host port identifier to the host.

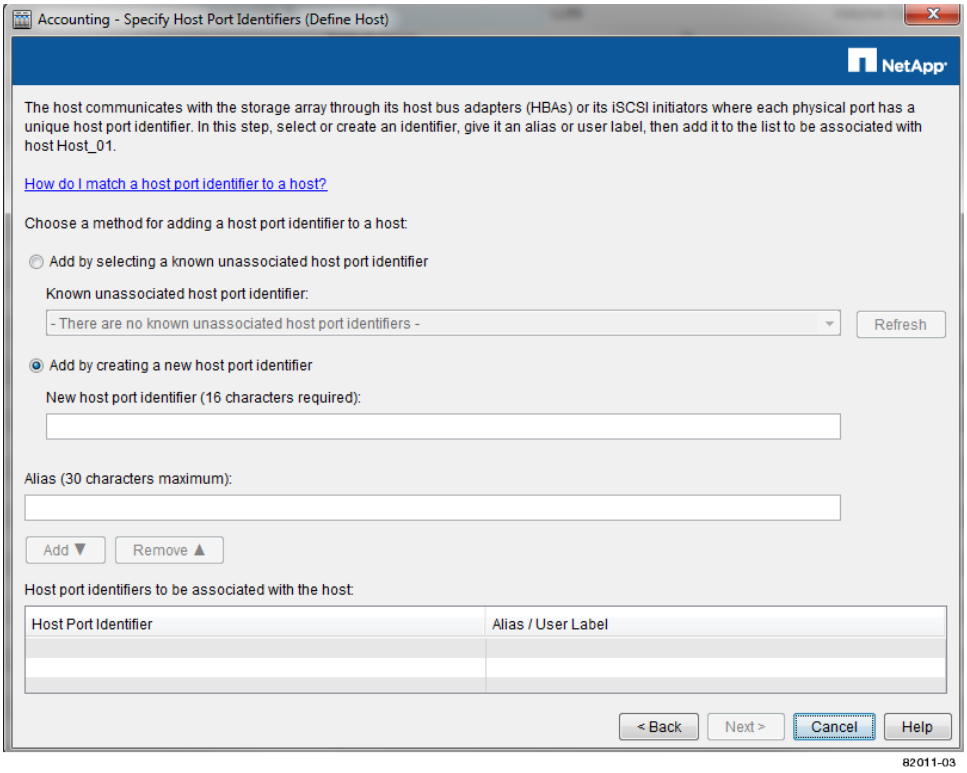
   You can add known unassociated host port identifiers by selecting the option **Add by selecting a known unassociated host port identifier**. From the drop-down list, select the identifier for the first port on the host.

   Note: The host port identifier is the World Wide Identifier (WWID). When the identifier is displayed in the selection list, the storage array can automatically detect the path to the host.

   If no identifiers are displayed, then there is an issue with the path to the host that must be resolved before the host can discover the storage. In this case, add new host port identifiers manually by

selecting the option **Add by creating a new host port identifier**. Enter the new host port identifier.

Note: Any path issues can be resolved after the host provisioning procedure is completed.



7. Enter a descriptive alias name for the host port identifier.

   Note: Alias names must not exceed 30 characters and cannot contain spaces. Names can contain letters, numbers, underscores (_), hyphens (-), and pound signs (#).

8. Select **Add** to add the host port identifier to the host.

9. Repeat Step *6* through Step *8* for each link between the host and the storage array.

   Note: Connect and provision two to four paths between any one host and the E-Series storage array.

10. Select **Next**.

11. From the **Host type (operating system)** drop-down list, select the operating system of the host.

12. Select **Next**.

13. Select **No – this host will NOT share access to the same volumes with other hosts**, then select **Next**.

14. Review the host definition information and confirm that the host name, the host type, and the host port identifiers are correct.

15. Select **Finish** to create the host.

16. Repeat Step *3* through Step *15* to create additional hosts as required.

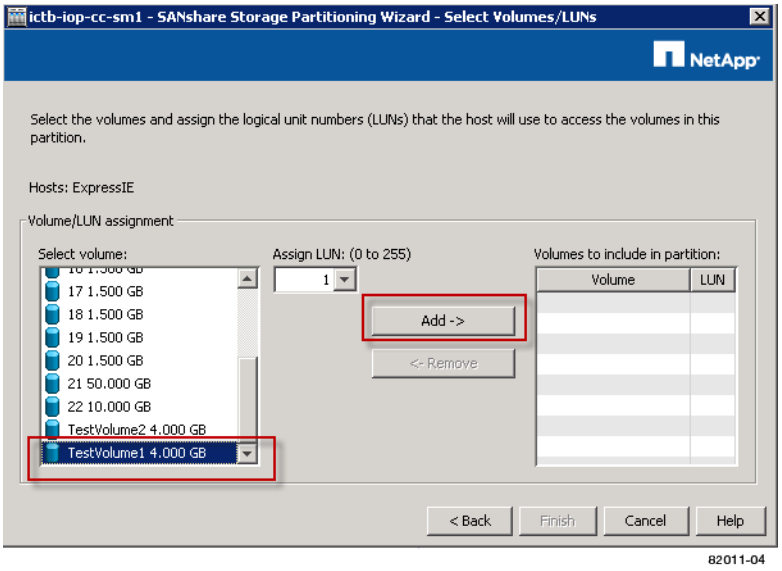
17. From the **Host Mappings** tab, review the storage array tree to verify that the hosts were created.

Mapping a volume to a host

Using SANtricity Storage Manager to create storage partitions, specify a volume to a Logical Unit Number (LUN), and map it to the host.

Steps

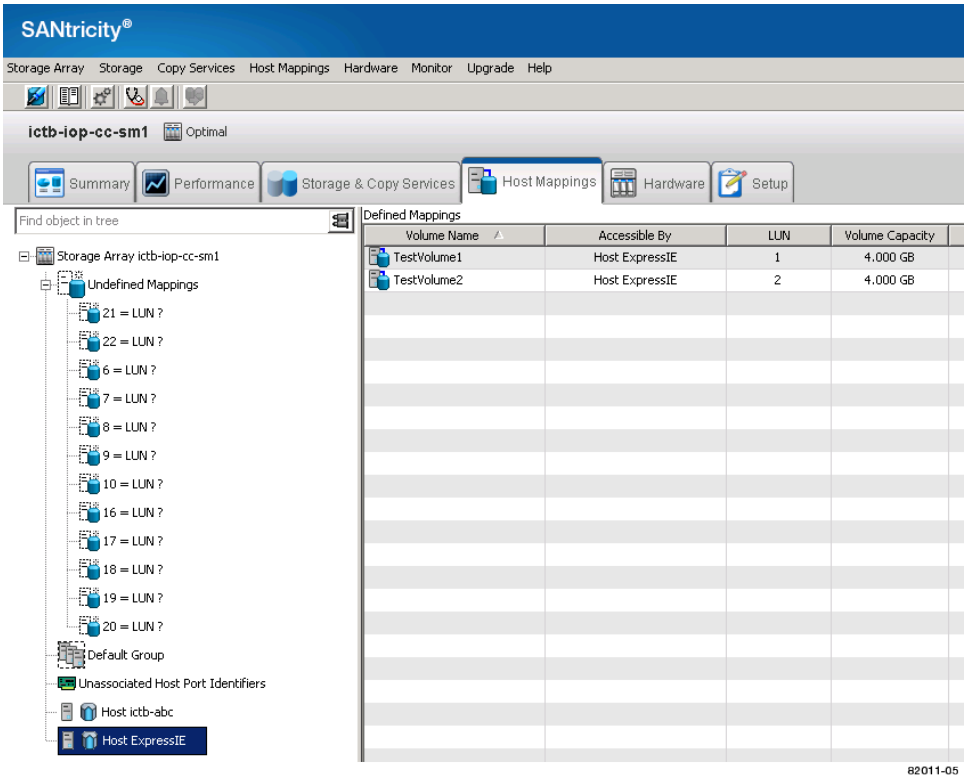
1. From the **Array Management Window (AMW)**, select the **Host Mappings** tab.
2. Select the storage array tree, right-click the desired host, and select **Define Storage Partition** to start the **SANshare Storage Partitioning** wizard.
3. On the **Welcome** page of the wizard, select **Next**.
4. Select **Host** to create a dedicated mapping, and then select the host name to be added to the partition.
5. Select **Next**.
6. Select an individual volume, assign a LUN number to the volume, and select **Add** to associate the volume (LUN) with the partition.



7. Repeat Step *6* until all desired volumes are added to the partition.
8. Select **Finish** to create the partition.
9. Review the storage array tree on the **Host Mappings** tab to confirm that the partition was successfully created.

Example

Note: In this example, the volume `TestVolume1` and `TestVolume2` are mapped to the host `Host ExpressIE`. Only this host has access to `TestVolume1` and `TestVolume2`. In the left pane of the screen, the storage partition on the host is indicated by the blue slice on the storage cylinder icon.


SANtricity®
Storage Array Storage Copy Services Host Mappings Hardware Monitor Upgrade Help
ictb-iop-cc-sm1 Optimal
Summary Performance Storage & Copy Services Host Mappings Hardware Setup
Find object in tree
Storage Array ictb-iop-cc-sm1
Undefined Mappings
21 = LUN ?
22 = LUN ?
6 = LUN ?
7 = LUN ?
8 = LUN ?
9 = LUN ?
10 = LUN ?
16 = LUN ?
17 = LUN ?
18 = LUN ?
19 = LUN ?
20 = LUN ?
Default Group
Unassociated Host Port Identifiers
Host ictb-abc
Host ExpressIE
Defined Mappings
Volume Name
Accessible By
LUN
Volume Capacity
TestVolume1
Host ExpressIE
1
4.000 GB
TestVolume2
Host ExpressIE
2
4.000 GB
82011-05

Discovering mapped storage on the host

After mapping volumes to the host, you must perform a rescan so that the host properly detects and configures it for multipathing.

Before you begin

You must have created one or more volumes and mapped them to the ESXi host. If using a vCenter Server, you must have added the host to its inventory. You must be using the vSphere Client or the vSphere Web Client to connect to the vCenter Server or to the ESXi host directly.

About this task

By default, an ESXi host automatically performs a periodic rescan every 5 minutes. Between the time a volume is created and mapped to a host, a volume might appear before a manual rescan is peformed. You can perform a manual rescan regardless to ensure all volumes are configured properly.

- Refer to the following VMware KB for instructions on how to perform a rescan of the storage on an ESXi host.

  http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1003988

Configuring storage on the host

Storage assigned to an ESXi host can be used either as a VMFS datastore or RDM.

Before you begin

The volumes mapped to the ESXi host must have been discovered properly.

About this task

All 5.x versions of ESXi support VMFS versions 5 and 3. You must use VMFS version 5 unless the datastore must also be used by an ESX/ESXi 4.x host, which supports only VMFS version 3.

Choices

- For instructions on creating VMFS datastores using either the vSphere Client or the vSphere Web Client, refer to the following VMware documentation page:

  http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.storage.doc%2FGUID-7BED10DD-3EF2-4670-BA7F-0EEB4EC6EB85.html

- For instructions on using volumes as RDMs using either the vSphere Client or the vSphere Web Client, refer to the following VMware documentation pages:

  - vSphere Client: *http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-8E664A67-26FC-4B20-920B-45DA8938D9F6.html*
  - vSphere Web Client: *http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-4236E44E-E11F-4EDD-8CC0-12BA664BB811.html*

Verifying storage access on the host

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

Before you begin

Verify that the volume has been used as a VMFS datastore or has been mapped directly to a VM for use as a RDM.

If the volume has been used as a VMFS datastore

Steps

1. In the navigation pane of the vSphere Client, select the host.
2. On the **Configuration** tab, select **Storage**.
3. Right-click the new datastore, and select **Browse Datastore**. The datastore browser is then displayed.
4. Using the datastore browser, create a new folder in the datastore and upload a file to the new folder.

After you finish

Remove the file and folder that were created.

If the volume has been assigned to a VM as an RDM

Steps

1. Create a filesystem on the volume in the Guest OS.
2. Create a new file in the new filesystem.
3. Force a controller failover, preferably by pulling all cables from one controller, and verify that you can still access the files on the LUN. Reset the storage to an optimal state when finished.

After you finish

Remove the file and folder that were created.

Where to find additional information

There are additional documents to help you learn more. All of the following documentation is available from the NetApp Support Site: *http://mysupport.netapp.com*.

Software Installation Reference for SANtricity Storage Manager 11.20

Provides reference configuration and software installation instructions for SANtricity Storage Manager 11.20. Covers less common configurations such as installation on the Solaris O/S, installation on a boot device, and Windows Server Core installation.

Multipath Drivers Guide for SANtricity Storage Manager 11.20

Describes how to install and operate the multipath drivers for SANtricity Storage Manager 11.20.

SANtricity Online Help

Describes how to use SANtricity Storage Manager to complete configuration and storage management tasks. Available within the product and as a PDF download.

NetApp Knowledgebase

(A database of articles) Provides troubleshooting information, FAQs, and instructions for a wide range of NetApp products and technologies.

VMware Configuration Maximums

vSphere 5.5 - *https://www.vmware.com/pdf/vsphere5/r55/vsphere-55-configuration-maximums.pdf*

vSphere 5.1 - *https://www.vmware.com/pdf/vsphere5/r51/vsphere-51-configuration-maximums.pdf*

vSphere 5.0 - *https://www.vmware.com/pdf/vsphere5/r50/vsphere-50-configuration-maximums.pdf*

Other VMware Publications

https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html

Copyright information

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S.

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

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

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

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

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

How to send comments about documentation and receive update notifications

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

If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

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

You can also contact us in the following ways:

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