SANtricity® Storage Manager 11.25 Express Guide

For Linux and InfiniBand
### Contents

Deciding whether to use this guide ................................................................. 4
Configuration and provisioning workflow ......................................................... 5
Verifying the configuration is supported .......................................................... 6
Filling out the worksheet (SRP protocols) ......................................................... 8
Filling out the worksheet (iSER protocols) ....................................................... 9
Installing and configuring SANtricity Storage Manager ..................................... 12
  Configuring IP addresses ............................................................................. 13
  Adding a storage array to SANtricity Storage Manager .................................. 14
Configuring the multipath software ................................................................. 18
Getting identifiers (SRP only) ........................................................................ 19
Installing and configuring Linux Unified Host Utilities 7.0 .............................. 20
Configuring the switches ............................................................................... 21
Configuring InfiniBand (SRP protocols) ......................................................... 22
Configuring InfiniBand (iSER protocols) ....................................................... 24
  Configure the storage array with iSER networking ........................................ 24
  Configure Storage Attached Hosts with iSER networking .............................. 24
Deciding whether to use a disk pool or a volume group .................................. 28
Creating a disk pool ....................................................................................... 29
Creating a volume group ............................................................................... 31
Creating a volume ......................................................................................... 33
  Creating a volume from a disk pool .............................................................. 35
  Creating a volume from a volume group ...................................................... 35
Defining a host in SANtricity Storage Manager .............................................. 37
Mapping a volume to a host ........................................................................... 39
Discovering mapped storage on the host ......................................................... 41
Configuring storage on the host .................................................................... 42
Verifying storage access on the host ............................................................... 43
Where to find additional information ............................................................. 44
Copyright information .................................................................................... 45
Trademark information ................................................................................... 46
How to send comments about documentation and receive update notifications .......................................................................................... 47
Deciding whether to use this guide

The "express method" for installing SANtricity Storage Manager software is appropriate for setting up a standalone Linux host to E-Series or EF-Series storage systems. It is designed to get the storage system up and running as quickly as possible with minimal decision points. This method includes: 1) setting up InfiniBand (IB) with the SCSI RDMA Protocol (SRP) or with the iSCSI Extensions for RDMA (iSER) protocol; 2) provisioning a LUN; and 3) making the LUN available using an InfiniBand host channel adapter (HCA) on a Linux host.

This guide does not provide information about data storage concepts or all the available options for installing and configuring the storage system.

This guide is based on the following assumptions:

- You have installed your storage array hardware.
- You have installed all other hardware and made the necessary connections.
- You are using out-of-band management.
- You are using a separate station for management rather than the data (I/O attached) host.
- During SANtricity configuration, you plan to attach the management station to the same subnet as the storage management ports.
- You know which protocol your host interface card (HIC) uses. You will configure storage in a Linux IB environment that includes either a 40 Gb/s HIC using the SRP protocol or a 56 Gb/s HIC using the SRP or iSER protocol.
- You are using NetApp supported IB HCAs and switches.
- You have reserved at least one static IP address for each NetApp controller on a 1 Gb/s management network.
- You are not configuring the data (I/O attached) host to boot from SAN.
- You are not using Linux as a virtualized guest.
- You are not using shared volumes.
- You have installed the host operating system.

If these assumptions are not correct for your installation, or if you want more conceptual background information, see the documentation listed in the Related information section. For topics related to the SANtricity Storage Manager software, see the SANtricity Online Help systems for the Enterprise Management Window (EMW) and the Array Management Window (AMW).

Related information

NetApp E-Series and EF-Series Systems Documentation Center
NetApp Interoperability Matrix Tool
SANtricity Storage Manager 11.25 Multipath Drivers Guide
SANtricity Storage Manager 11.25 Software Installation Reference
Hardware Cabling Guide
Configuration and provisioning workflow

When you make storage available to a host using the SRP or iSER protocol, you provision a volume in SANtricity Storage Manager, and then map the volume to a host or host group.
Verifying the 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. Use the Component Explorer in the left panel to select the following components:
   - Host OS version
   - Host computer CPU architecture (for standard rack servers)
   - Protocol
   - Host channel adapter (HCA) component
   - HCA firmware
   - Open Fabrics Enterprise Distribution (OFED) version
   - Host multipath (inbox Device Mapper Multipath or DM-MP)

3. Select the Show Results button.
   A matrix of possible configurations is displayed. The Status column indicates whether each configuration is supported.

4. Select the configuration link in the Name column.
   The Configuration Details window displays information for each component.

5. Review the information in the following tabs in the Configuration Details window:
   - Notes: Lists important information specific to your configuration. Review the alerts to identify the hot fixes that are required for your operating system.
• **Policies & Guidelines**: Provides general guidelines for all SAN configurations.

6. Update HCA driver, firmware, and bootcode as necessary.

**Related information**

*NetApp Interoperability Matrix Tool*
Filling out the worksheet (SRP protocols)

As you progress through this guide, you can use this worksheet to record storage configuration information. You will need this information to perform provisioning tasks.

**Note:** If your configuration includes a host interface card using the SRP protocol, use this worksheet. If your configuration uses the iSER protocol, use the worksheet in *Filling out the worksheet (iSER protocols)* on page 9.

---

**SRP: Host identifiers**

**Note:** The initiator GUIDs are determined in the task, *Getting identifiers (SRP only)* on page 19.

<table>
<thead>
<tr>
<th>Callout No.</th>
<th>Host (initiator) port connections</th>
<th>GUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Host</td>
<td><em>not applicable</em></td>
</tr>
<tr>
<td>3</td>
<td>Switch</td>
<td><em>not applicable</em></td>
</tr>
<tr>
<td>4</td>
<td>Target (storage array)</td>
<td><em>not applicable</em></td>
</tr>
<tr>
<td>2</td>
<td>Host port 1 to IB switch 1 (&quot;A&quot; path)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Host port 2 to IB switch 2 (&quot;B&quot; path)</td>
<td></td>
</tr>
</tbody>
</table>

---

**SRP: Recommended configuration**

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

---

**SRP: Mapping host name**

**Note:** The mapping host name is created during the workflow, *Defining a host in SANtricity Storage Manager* on page 37.

<table>
<thead>
<tr>
<th>Mapping host name</th>
<th>Host OS type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Filling out the worksheet (iSER protocols)

As you progress through this guide, you can use this worksheet to record storage configuration information. You will need this information to perform provisioning tasks.

**Note:** If your configuration includes a host interface card using the iSER protocol, use this worksheet. If your configuration uses the SRP protocol, use the worksheet in *Filling out the worksheet (SRP protocols)* on page 8.

**iSER: Host identifiers**

**Note:** The software initiator IQN is determined during the task, *Configure Storage Attached Hosts with iSER networking* on page 24. You will use this information in the topics, *Defining a host in SANtricity Storage Manager* on page 37 and *Configure Storage Attached Hosts with iSER networking* on page 24.

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

<table>
<thead>
<tr>
<th>Callout No.</th>
<th>Host port connections</th>
<th>Software initiator IQN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Host (initiator) 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>[ ]</td>
<td></td>
</tr>
</tbody>
</table>

**iSER: Recommended configuration**

Recommended configurations consist of two host (initiator) ports and four target ports.
**iSER: Target IQN**

Document the target IQN for the storage array. You will use this information in *Configure Storage Attached Hosts with iSER networking* on page 24.

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

<table>
<thead>
<tr>
<th>Callout No.</th>
<th>Array name</th>
<th>Target IQN</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Array controller (target)</td>
<td></td>
</tr>
</tbody>
</table>

**iSER: 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 Attached Hosts with iSER networking* on page 24.

**Subnet A**

Define the subnet to be used.

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Callout No.</th>
<th>Array controller (target) port connections</th>
<th>IQN</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Switch</td>
<td>not applicable</td>
</tr>
<tr>
<td>5</td>
<td>Controller A, port 1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Controller B, port 1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Host 1, port 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Host 2, port 1</td>
<td></td>
</tr>
</tbody>
</table>

**Subnet B**

Define the subnet to be used.

<table>
<thead>
<tr>
<th>Network Address</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Callout No.</th>
<th>Array controller (target) port connections</th>
<th>IQN</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Switch</td>
<td>not applicable</td>
</tr>
<tr>
<td>10</td>
<td>Controller A, port 2</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Controller B, port 2</td>
<td></td>
</tr>
<tr>
<td>Callout No.</td>
<td>Array controller (target) port connections</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Host 1, port 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Optional) Host 2, port 2</td>
<td></td>
</tr>
</tbody>
</table>

**iSER: Mapping host name**

**Note:** The mapping host name is created during the workflow, *Defining a host in SANtricity Storage Manager* on page 37.

<table>
<thead>
<tr>
<th>Mapping host name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Host OS type</td>
<td></td>
</tr>
</tbody>
</table>
Installing and configuring SANtricity Storage Manager

When you install the SANtricity Storage Manager software on your management station, a graphical user interface (GUI) and a command line interface (CLI) are installed by default. These instructions assume you will install the SANtricity Storage Manager GUI on a management station and not on the I/O host.

Before you begin

- You must have the correct administrator or superuser privileges.
- You must ensure the system that will contain the SANtricity Storage Manager client has the following minimum requirements:
  - **RAM**: 2 GB for Java Runtime Engine
  - **CPU**: Confirm that your host's architecture is supported. Use the *NetApp Interoperability Matrix Tool*.
  - **Disk space**: 5 GB

About this task

You will install the SANtricity Storage Manager software on the management station. This section 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.

For more information about installation methods and customizations, see the *SANtricity Storage Manager Software Installation Reference*.

Steps

1. Download the SANtricity software release from the *NetApp Support* site.
2. Run the SANtricity installer.

<table>
<thead>
<tr>
<th>Windows</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Double-click the SMIA*.exe install package to start the installation.</td>
<td>a. Go to the directory where the installation package SMIA*.exe is located.</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>c. Run the chmod +x SMIA*.bin command to grant execute permission to the file.</td>
</tr>
<tr>
<td></td>
<td>d. Run the ./SMIA*.bin command to start the installer.</td>
</tr>
</tbody>
</table>

3. Use the installation wizard to install the software on the management station.
### Configuring IP addresses

In this best-practices method for configuring communications, you configure the management station and array controllers to reside on the same private network.

#### Steps

1. Connect an Ethernet cable to the management station and to management port 1 on controller A or B. Wait 3 minutes for DHCP addressing to time out.

   **Note:** Do not use port 2 on either controller. These ports are reserved for use by NetApp technical personnel.
2. Follow these steps to temporarily change the IP address of 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. You will revert back to this IP address after you have completed the procedure.

   b. Change the settings on the management station so that it is on the same private network as the controllers, which have these default IP addresses in an IPv4 network:

      Controller A, port 1: 192.168.128.101
      Controller B, port 1: 192.168.128.102

      Set the IP address for the management station to something other than the controller IP addresses. For example, for an IPv4 network, use 192.168.128.100 for the management station; for an IPv6 network, use FE80:0000:0000:0000:02A0:B8FF:FE29:1D7C.

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

   c. If your network is an IPv4 network, check the subnet mask to verify that it is set to the default setting:

      255.255.255.0

   d. From a command prompt on the management station, ping the IP address of the controller connected to the management station to make sure it is accessible.

   **Example**

   ```
   > ping 192.168.128.101 <or 192.168.128.102>
   Reply from 192.168.128.101 <or 102>: bytes=32 time<1ms TTL=64
   Ping statistics for 192.168.128.101 <or 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
   ```

**Adding a storage array to SANtricity Storage Manager**

After you have configured the private network between the management station and the array controllers, you add the controller to SANtricity Storage Manager using the Enterprise Management Window (EMW).

**Steps**

1. Open SANtricity Storage Manager. The steps you use depend on the operating system of your management station.

   • If you use a Windows management station, open SANtricity Storage Manager from the Windows Start menu. The (EMW) is displayed.

   • If you use a Linux management station, use a Linux terminal window. Run the SMclient command from any directory. The Linux installation also places a shortcut to launch SANtricity Storage Manager on the desktop. After using the SMclient command or the shortcut to open the SANtricity Storage Manager, the (EMW) is displayed.

2. On the Select Addition Method screen, select the Manual radio button, and then select OK.
**Note:** When you open SANtricity Storage Manager for the first time, the Select Addition Method screen prompts you to select the Automatic or Manual method to add a new storage array.

3. 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 default IP address of port 1 for the controller connected to the management station (controller A or B). The default addresses are:

      Controller A, port 1: 192.168.128.101
      Controller B, port 1: 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 another storage array. 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. You can use this wizard 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, you should create disk pools using a different procedure, described in *Creating a disk pool* on page 29.

4. 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.

5. Name the storage array so you can find it more easily in the EMW after you change the IP addresses:
   a. In the Setup tab, select Name/Rename Storage Arrays.
   b. In the Select storage array: list, confirm that the storage array you added is selected.
   c. In the Storage array name field, type a name for the storage array.
   d. Select OK.
   e. On the Name/Rename Storage Arrays warning dialog, select Yes to dismiss the warning and continue.

6. Configure the network configuration information of the controllers, using information you obtain from your network administrator.
   a. Select the Hardware tab in the Array Management Window (AMW).
   b. Select the visual representation of one of the controllers in the Hardware tab.
   c. Right-click, and then select 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 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 Steps 6.e through 6.g.
6. Select OK.

j. Close the AMW.

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

8. Disconnect the private network and reconnect into your regular LAN.
   a. Disconnect the management station from the controller and reconnect it into your LAN.
   b. Change the management station to use the original IP address. Refer to your operating system documentation for instructions on how to change the network settings on the management station and how to verify that the address has changed.
   c. Connect the controller into your LAN.

9. 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 6.
   d. Select **Add**.
   e. On the **Storage Array Added** screen, select **Yes** to add another storage array. Otherwise, select **No**.

10. Find the IQNs of the controller host ports.
    a. Click the **Setup** tab.
    b. Click the link for **Manage iSCSI Settings**. Scroll through the information to find the IQNs.
    c. Record the IQNs in the worksheet.
Configuring the multipath software

If a disruption of one or more physical paths occurs, the multipath software maintains an active path to the underlying network storage. 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.

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. Example: `# systemctl start multipathd`

4. Configure multipath for startup persistence. Example: `# chkconfig multipathd on`
   
   For additional configuration details, see the SANtricity Storage Manager Multipath Drivers Guide.

Related information

   SANtricity Storage Manager 11.25 Multipath Drivers Guide
Getting identifiers (SRP only)

About this task

The InfiniBand-diags package includes commands to display the globally unique ID (GUID) of each InfiniBand 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. Use the worksheet for SRP protocols to record the initiator’s GUIDs.
Installing and configuring Linux Unified Host Utilities 7.0

Linux Unified Host Utilities 7.0 includes tools to manage NetApp storage, including failover policies and physical paths.

About this task
See the *Linux Unified Host Utilities 7.0 Installation Guide*.

Steps
1. Use the *NetApp Interoperability Matrix Tool* to determine the appropriate version of Unified Host Utilities 7.0 to install.
   The versions are listed in a column within each supported configuration.
2. Download the Unified Host Utilities 7.0 from *NetApp Support*.

Related information
   *Linux Unified Host Utilities 7.0 Installation Guide*
   *NetApp Interoperability Matrix Tool*
   *NetApp Support*
Configuring the switches

Before you begin
You must have administrator credentials for the switches.

About this task
InfiniBand fabrics require that a subnet manager is running somewhere on the fabric. If switches are available, enable the subnet manager using the management interface for the switches. If switches are not available, run a subnet manager on a host in the fabric.

For details about enabling the subnet manager, see the switch vendor's documentation.

Steps
1. Log in to the InfiniBand switch administration program.
2. Enable the subnet manager and save the configuration.
Configuring InfiniBand (SRP protocols)

About this task

Note: If your configuration uses the SRP protocol, follow the steps in this section. If your configuration uses the iSER protocol, go to the section, Configuring InfiniBand (iSER protocols) on page 24.

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

Steps

1. Install the OFED/RDMA driver stack for your OS.
2. Configure OFED/RDMA to load the SRP module.
3. In the OFED/RDMA configuration file, set SRP_LOAD=yes and SRP_DAEMON_ENABLE=yes.
4. Enable and start the OFED/RDMA service.

   For RHEL
   • To enable the InfiniBand modules to load on boot:
     
```bash
chkconfig rdma on
```

   • To load the InfiniBand modules immediately:

```
service rdma start
```

   For SUSE Linux
   • To enable the InfiniBand modules to load on boot:

```
chkconfig openibd on
```

   • To load the InfiniBand modules immediately:

```
service openibd start
```

5. Enable the SRP daemon.

   For RHEL
   • To enable the SRP daemon to start on boot:

```
chkconfig srpd on
```

   • To start the SRP daemon immediately:

```
service srpd start
```

   For SUSE Linux
• To enable the SRP daemon to start on boot:

    \texttt{chkconfig opensmd on}

• To start the SRP daemon immediately:

    \texttt{chkconfig opensmd start}

\textbf{Related information}

\textit{NetApp Interoperability Matrix Tool}
Configuring InfiniBand (iSER protocols)

Note: If your configuration uses the iSER protocol, follow the steps in this section. If your configuration uses the SRP protocol, go to the section, Configuring InfiniBand (SRP protocols) on page 22.

Configure the storage array with iSER networking

About this task

When you are using a 56-Gb/s HIC with the iSER protocol, additional array configuration is required.

Steps

1. From the Setup tab, select Configure iSCSI Host Ports to set the storage array iSCSI addresses.
   
   Put the array iSCSI addresses on the same subnet as the host port(s) you will use to create iSCSI sessions. For addresses, see Filling out the worksheet (iSER protocols) on page 9.

2. From the Devices tab, select the storage array and go to iSER > Manage Settings to find the IQN.
   
   This information may be necessary when you create iSER sessions from operating systems that do not support send targets discovery. Enter this information in the worksheet, in Filling out the worksheet (iSER protocols) on page 9.

Configure Storage Attached Hosts with iSER networking

About this task

The InfiniBand OFED driver stack supports running both iSER and SRP simultaneously on the same ports, so no additional hardware is required. Before starting this step, see the Interoperability Matrix to ensure that a NetApp-recommended OFED is installed on the system.

Steps

1. Enable and start iSCSI services on the host(s):
   
   For RHEL
   
   ```
   chkconfig iscsi on
   chkconfig iscsid on
   ```

   For SUSE Linux
   
   ```
   chkconfig open-iscsi on
   ```

2. Configure IPoIB network interfaces:
   
   a. Identify the InfiniBand ports that will be used. Document the HW Address (MAC address) of each port. Document the addresses in the worksheet: Filling out the worksheet (iSER protocols) on page 9.
b. (Optional; recommended) Configure persistent names for the InfiniBand network interface devices.

c. Configure the IP address and network information for the IPoIB interfaces identified. The specific interface configuration required may vary depending on the operating system used. Consult your vendor’s operating system documentation for specific information on implementation.

**Example**

For RHEL 6.x Interface Name ib0, edit the `/etc/sysconfig/network-scripts/ifcfg-ib0` configuration file.

```plaintext
ONBOOT=yes
Name=ib0
Type=InfiniBand
IPADDR=192.168.xx.yy
PREFIX=24
DEFROUTE=no
HWADDR=<Port 0 HW Address Here>
```

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

**Example**

```
#service network restart
```

e. Verify connectivity to the target ports. From the host, ping the IP addresses you configured in Configure the storage array with iSER networking on page 24.

3. Restart services to load the iSER module. 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.

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

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

5. Create iSCSI session configurations:
   a. Create iface configuration files for each InfiniBand interface.

**Example**

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

```plaintext
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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>iface.net_ifacename</td>
<td>The interface device name (ex. ib0).</td>
</tr>
</tbody>
</table>
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.

• **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. (This method does not work on RHEL 6.6 or SLES 11.3 or older. For RHEL 6.6 or SLES 11.3 or older, use Method 2.)

```
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, navigate to the **Storage Array** > **iSER > View/End Sessions**.

**Related information**

*NetApp Interoperability Matrix Tool*
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 your key storage requirements, such as expected I/O workload, performance requirements, and data protection requirements.

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

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

After you have made your decision, go to either Creating a disk pool on page 29 or Creating a volume group on page 31 to continue.

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

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

About this task

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

Steps

1. From the **Array Management Window 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.
   b. Select whether you want to see any available drives, or just secure-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, such as 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 to verify the disk pool was created.

6. Go to Creating a volume on page 33.

Related information

SANtricity Storage Manager 11.25 Software Installation Reference
Creating a volume group

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

About this task

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

Steps

1. Verify that hot spare coverage is adequate for the storage array.
   
   a. From the **Array Management Window**, select **Hardware > Hot Spare Coverage**.
   
   b. On the **Hot Spare Drive Options** dialog box, select **View/change current hot spare coverage** and select **OK**.
   
   c. On the **Hot Spare Coverage** dialog box, view coverage. 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 help determining if coverage is adequate, select the hyperlink “Tips on providing hot spare coverage” on the Hot Spare Coverage dialog box.

   d. Select **Close**.

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

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

3. On the **Introduction** page of the wizard, select **Next**.

4. On the **Volume Group Name & Drive Selection** page of the wizard, perform the following steps:
   
   a. Enter a name for the new volume group.
   
   b. Select the **Automatic (Recommended)** radio button from the **Drive selection choices** list, and then select **Next**.

5. On the **RAID Level and Capacity** page, perform the following steps:
   
   a. Select the desired RAID level for the new volume group from the drop-down list.

      **Note:** For help determining the best RAID level, select the hyperlinks “What RAID level is best for my application?” and “What is tray loss protection?” on the RAID Level and Capacity page.
   
   b. Select the desired volume group configuration from the list of available configurations and select **Finish**.
   
   c. The **volume group** wizard automatically displays a prompt for you to create a volume in the newly created volume group. To create a volume immediately, select **Yes** to continue with the volume creation. Go to **Creating a volume** on page 33.
Related information

SANtricity Storage Manager 11.25 Software Installation Reference
Creating a volume

Using SANtricity Storage Manager, you create a volume—a single accessible storage area—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
You must have determined 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 you want to create the new volume.

2. Right-click Free Capacity > Create Volume.
   If you are creating a volume on a disk pool, the following dialog box appears.

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

If you are creating a volume on a volume group, the following dialog box appears.
3. Configure the volume parameters.

Onscreen flyovers provide 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** check box.

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

b. From the **Units** drop-down list, select the appropriate unit for the new volume capacity.

c. Specify the volume capacity to be taken from the free capacity that is listed.

d. Enter the volume name.

e. From the **Map to host** drop-down list, select the **Map later** option.

4. Specify the Quality of Service attributes. Use the onscreen flyovers and the SANtricity Online Help to get more information about particular attributes.

   **Note:** The **Use SSD cache** check box is not available in the Quality of Service section because you have chosen to map the volume to a host later. See the Array Management Window Online
Help topic “Learn about SSD Cache” to decide if it is appropriate to enable SSD cache 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 check box.

   This check box appears only if the drives, the controller, and the host bus adapter are all DA-capable.

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 (see Creating a volume from a disk pool) or a volume group (see Creating a volume from a volume group).

Creating a volume from a disk pool

After you have started creating a volume from the free capacity of a disk pool, you complete the volume creation by specifying if you want to enable dynamic cache read prefetch.

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 33.

Steps

1. Select the Enable dynamic cache read prefetch check box to enable it.

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

2. Select Finish.

Creating a volume from a volume group

After you have started creating a volume from the free capacity of a volume group, you complete the volume creation by specifying how the volume will be used. Setting the correct usage type helps ensure the best performance.

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 33.

Steps

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

   • Select File system, Database, or Multimedia to have the optimal segment size and cache settings automatically configured for the best performance.

   • For less common volume usages, select Custom from the Volume I/O characteristics type drop-down list. If appropriate for your environment, select the Enable dynamic cache read prefetch check box. Select the appropriate segment size from the Segment size list. See the SANtricity Online Help to learn more about performance tuning.

2. Select Finish.

   You are prompted to create another volume.
3. Select **Yes** to create another volume or **No** to finish creating the volume.
Defining a host in SANtricity Storage Manager

Using SANtricity Storage Manager, you allow the volumes to be shared with the host.

About this task
You define a new logical host on the storage array so that volumes can be shared with the host.

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.
   b. In the Question area of the dialog box, keep the Yes selected.
4. Select Next.
5. If the controller supports multiple host interface types, select one type from the Choose a host interface type drop-down list.
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 iSCSI Qualified Name (IQN). 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, there is an issue with the path to the host, and the storage cannot be discovered. Resolve the host issue, then change the host port identifier that was not discovered by selecting the option Add by creating a new host port identifier. Enter the new host port identifier.
Enter a descriptive alias name for the host port identifier.

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

Repeat Step 6 through Step 8 for each link between the host and the storage array. You can connect and provision two to four paths between any one host and the E-Series storage array. Additional links between host and storage will not show up as different identifiers; they will all exist behind the same IQN.

Select Next.

From the Host type (operating system) drop-down list, select host type Linux (DM-MP).

Select Next.

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

Note: These instructions assume a non-clustered configuration.

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

Select Finish to create the host.

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

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, you assign a logical unit number (LUN) to a volume and map the LUN 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 then 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 to the volume, and then select Add to associate the volume (LUN) with the partition.

   **Note:** When assigning LUNs for volumes attached to Linux hosts, start with LUN 1 rather than LUN 0. If an array is connected to the host before a device is mapped to LUN 0, the Linux host detects the REPORT LUNS well known logical unit as LUN 0, so that it can complete discovery. LUN 0 might not immediately map properly with a simple rescan, depending on the version of the host operating system.

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 volumes TestVolume1 and TestVolume2 are mapped to the 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.
Discovering mapped storage on the host

LUNs on your storage system appear as disks to the Linux host. When you add new LUNs, you must manually rescan the associated disks to discover them. The host does not automatically discover new LUNs.

Steps

1. Scan the LUNs by running the `# rescan-scsi-bus.sh` command from a terminal window on the host.
   
   This command works only if sg3_utils is installed. Alternatively, you can reboot the host or manually scan each SCSI host.

   ```
   # echo "- - -"
   > /sys/class/scsi_host/host3/scan
   ```

2. Verify disk discovery by running the `# multipath -ll` command.

Example

```
[root@localhost ~]# multipath -ll
360080e5000321bb800009b1535f887a dm-2 NETAPP ,INF-01-00
   size=25G features='4 queue_if_no_path pg_init_retries 50
   retain_attached_hw_handle'
   hwhandler='1 rdac' wp=rw
   `-+- policy='service-time 0' prio=14 status=active
     `- 12:0:0:0 sde 8:64 active ready running
   `-+- policy='service-time 0' prio=9 status=enabled
     `- 11:0:0:0 sdd 8:48 active ready running
```
**Configuring storage on the host**

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.

**Before you begin**

The host must have discovered the LUN.

In the /dev/mapper folder, run the ls command to see the available disks.

**About this task**

Use the multipath command to retrieve the SCSI ID of the mapped disk. 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.

You can initialize the disk as a basic disk with a GPT or MBR partition table.

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

**Steps**

1. 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).
   
   **Example**
   
   ```
   # parted -a optimal -s -- /dev/mapper/
   360080e5000321bb8000092b1535f887a mklable
   gpt mkpart primary ext4 0% 100%
   ```

2. Create a file system on the partition.
   
   The method for creating a file system varies depending on the file system chosen.
   
   **Example**
   
   ```
   # mkfs.ext4 /dev/mapper/360080e5000321bb8000092b1535f887a1
   ```

3. Create a folder to mount the new partition.
   
   **Example**
   
   ```
   # mkdir /mnt/ext4
   ```

4. Mount the partition.
   
   **Example**
   
   ```
   # mount /dev/mapper/360080e5000321bb8000092b1535f887a1 /mnt/ext4
   ```
**Verifying storage access on the host**

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

**Before you begin**
The LUN must be initialized and 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. Compare the copied files to the original.
   You can run the `diff` command to compare two files.
4. Run the `multipath -ll` command to view the paths to the LUN and verify that you have the expected number of paths (4).
5. Force a controller failover, preferably by pulling all cables from one controller, and then verify that you can still access the files on the LUN. When you are finished, reset the storage to an optimal state.
6. Run the `multipath -ll` command to view the paths to the LUN and verify that you have the expected number of paths (4).

**After you finish**
Remove the file and folder that you copied.
Where to find additional information

Use the resources listed here if you need additional information. You can also use the Online Help systems for the Enterprise Management Window (EMW) and the Array Management Window (AMW) of SANtricity Storage Manager.

- **SANtricity Storage Manager 11.25 Software Installation Reference** provides reference information about configuration and software installation. Covers less common configurations such as installation on a boot device and Windows Server Core.

- **SANtricity Storage Manager 11.25 Multipath Drivers Guide** describes how to install and operate the multipath drivers.

- **Linux Unified Host Utilities 7.0 Installation Guide** describes how to use the Linux Unified Host Utilities 7.0.

- 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.

**Related information**

- **NetApp E-Series and EF-Series Systems Documentation Center**
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