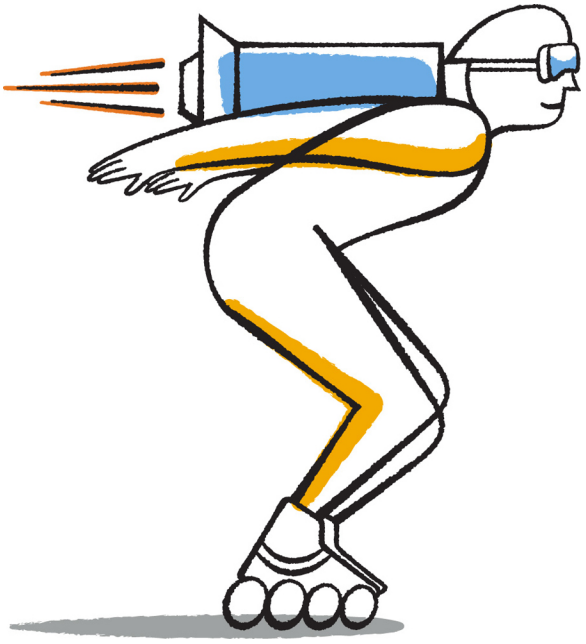
Clustered Data ONTAP® 8.3

Express Setup Guide for 80xx Systems



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: 215-09763_A0
January 2015

Contents

Deciding whether to use this guide

This guide describes how to quickly set up your FAS80xx series storage system for the first time, from opening the box to setting up the cluster in a NAS or SAN environment, using best practices and without a lot of background detail.

You should use this guide if you want to set up your system in the following way:

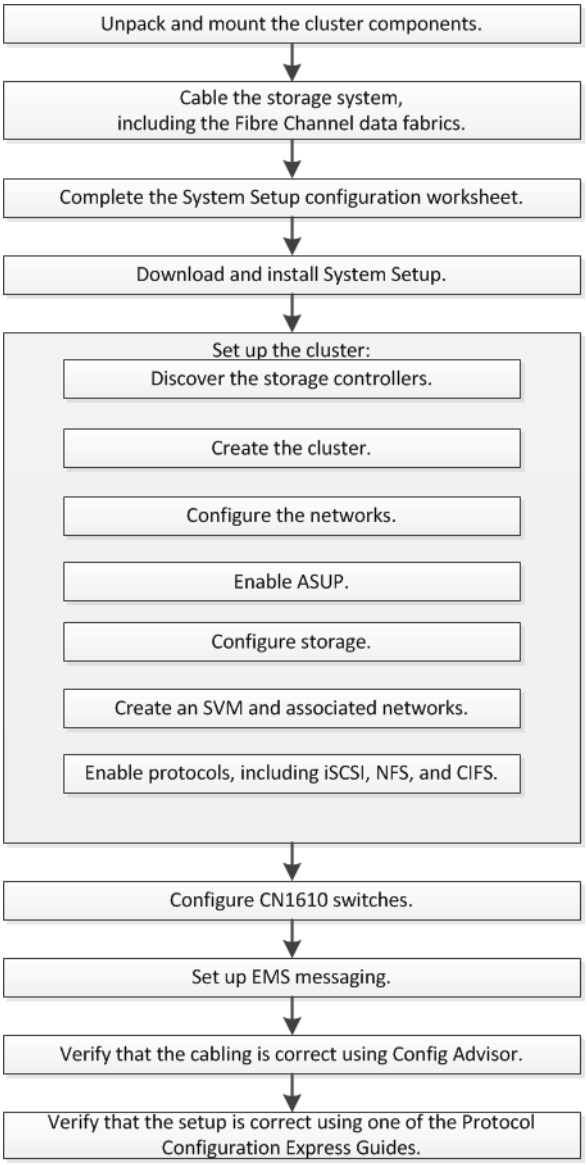
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to set up a 2-node switchless or 4-node switched cluster.
- You want to use System Setup, not the Data ONTAP command-line interface or an automated scripting tool.
- You are setting up your storage system for the first time and not upgrading or expanding your cluster.
- You want to use Config Advisor to verify that your cabling is correct.
- You are not using FCoE.
- You want System Setup to configure the basic setup for a test aggregate, so that you can use System Manager for additional configuration.
- You want System Setup to automatically reserve service processor IP addresses.

If these assumptions are not correct for your situation, you should see the following resources:

- *Clustered Data ONTAP 8.3 Software Setup Guide*
- *Clustered Data ONTAP 8.3 Upgrade and Revert/Downgrade Guide*
- *Installation and Setup Instructions FAS8020 systems*
- *Installation and Setup Instructions FAS8040/FAS8060 Systems*
- *Installation and setup Instructions FAS80xx Systems with I/O Expansion Modules*
- *NetApp Hardware Universe*
- *SAS Disk Shelves Universal SAS and ACP Cabling Guide*

FAS8000 setup workflow

Setting up an 80xx system involves cabling the physical components and setting up the cluster software. You should then configure your protocols and verify that the system is operating.



Steps

Unpacking the components

As you unpack the cluster components, it is important to track which disk shelves go with which storage controllers. Keeping track of this information and locating the disk shelves with their storage controllers simplifies cabling and ensures that each controller has its root volume and Data ONTAP software.

The factory labels the disk shelves with the storage controller to which they should connect.

Locating the disk shelves for each controller

Before mounting the components, you must locate the external disk shelves that belong to each controller. The factory installs the root volume and Data ONTAP software on one disk shelf for each controller. By cabling the correct disk shelves to each controller, you ensure that each controller has its root volume.

Before you begin

The components must not be in the rack or cabinet so that you can see the labels on the top of the component chassis.

About this task

Each external disk shelf has a sticker on the top of its chassis that lists the serial number of the controller to which the shelf connects. The sticker also lists the stack number for configurations with more than one stack of disk shelves per controller.

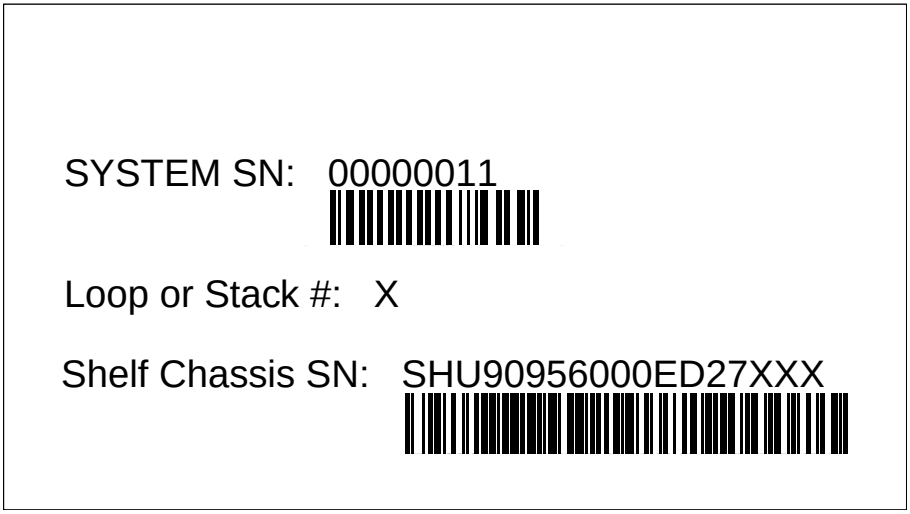
Steps

1. As you unpack the external disk shelves and storage controllers, check the labels on the top of each chassis.

The SYSTEM SN is the identifier of the storage controller and the Shelf Chassis SN is the identifier of the disk shelf.

2. Using the label information, group or mark the external disk shelves and controllers so that you can cable the disk shelves to the correct storage controllers after the components are mounted.

The following illustration shows an example of the label for external disk shelves:



Mounting the components

You should mount the components in the rack or cabinet in the recommended configurations to simplify cabling and service access.

Switched and switchless configurations

The following configurations are valid:

- Two-node or four-node switched clusters
  Always include the cluster interconnect, and optionally include management switches. For SAN access, optionally include FC switches.
- Two-node switchless clusters
  Do not include cluster interconnect or management switches. For SAN access, optionally include FC switches.

Note: If you ordered the cluster in NetApp cabinets, the components are already mounted. The disk shelf containing the root volume is mounted next to its storage controller.

Depending on the number of disk shelves and size of the rack or cabinet, you might require multiple racks or cabinets. The general rule is to keep the components of an HA pair together to simplify cabling.

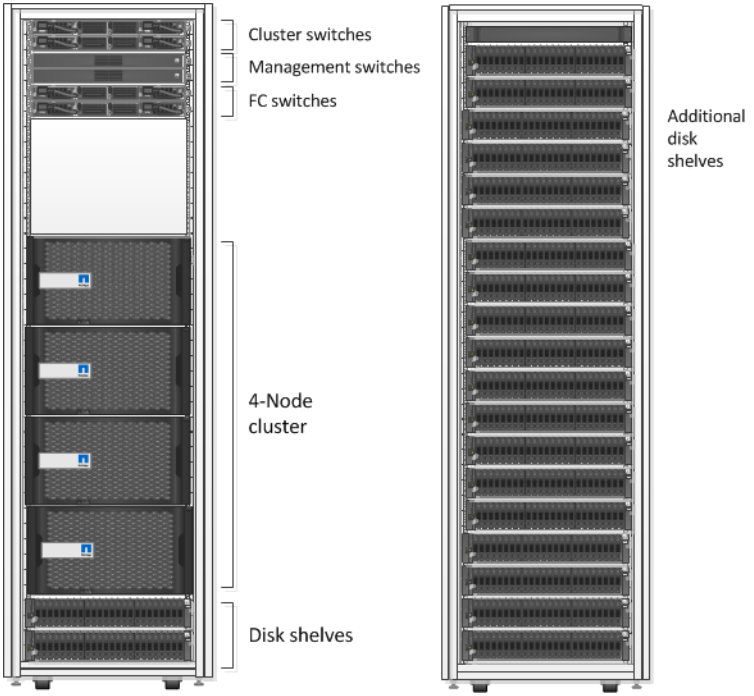
Each disk shelf has a label on the top of its chassis that lists the storage controller to which that disk shelf connects. Note that the label is not visible after mounting.

Typical configuration

The cabinet contains the switches (if applicable), the disk shelves, and the controllers. The components are installed as follows:

- Cluster switches, always at the top
- Optional management switches
- Optional FC switches
- Disk shelves, first HA pair
- Two to four nodes
- Disk shelves, second HA pair

Blank plates are installed to cover any empty spaces in the cabinet:



Cabling the 80xx system

Correctly cabling the system enables the components to communicate with each other and with the rest of your storage environment in both normal and failure conditions.

Labeling the cables

You should label the cables to simplify future expansion and to make troubleshooting of the cluster easier. You can use the binder of labels that is included in the accessories box.

About this task

You can label the cables at any time during the installation process.

Steps

1. Using the labels in the binder supplied, label each end of each cable as required by your environment.

   You do not need to label the power cables.

2. Save the binder containing any remaining labels for future expansion of the cluster.

Cabling the disk shelf alternate control path ports

The alternate control path (ACP) uses the ACP ports on the disk shelves to connect to the storage controllers. Having a control path that is separate from the data path increases reliability and simplifies troubleshooting.

About this task

The ACP cabling uses standard CAT6 Ethernet cables.

Steps

1. Connect the private management port e0P of controller 1 in an HA pair to the ACP port with the square symbol on the first disk shelf.

   The e0P port is labeled with a wrench and padlock symbol ().

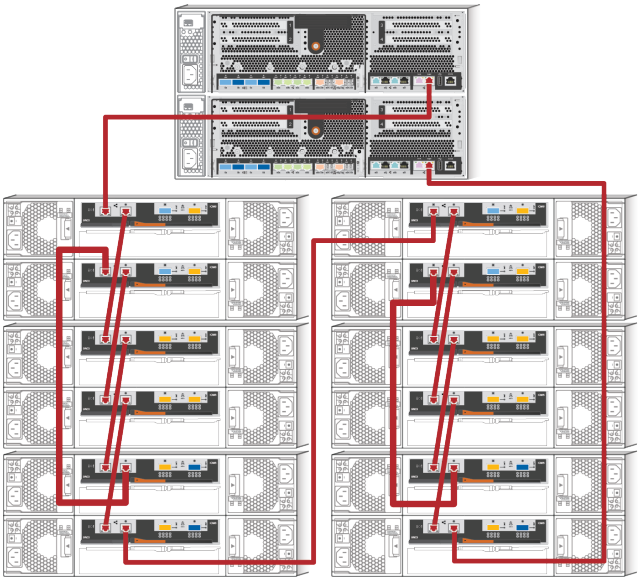
2. Connect the ACP port with the round symbol to the next ACP port with a square symbol.

   Continue in a daisy chain until all ACP ports for the shelves used by the HA pair are connected.

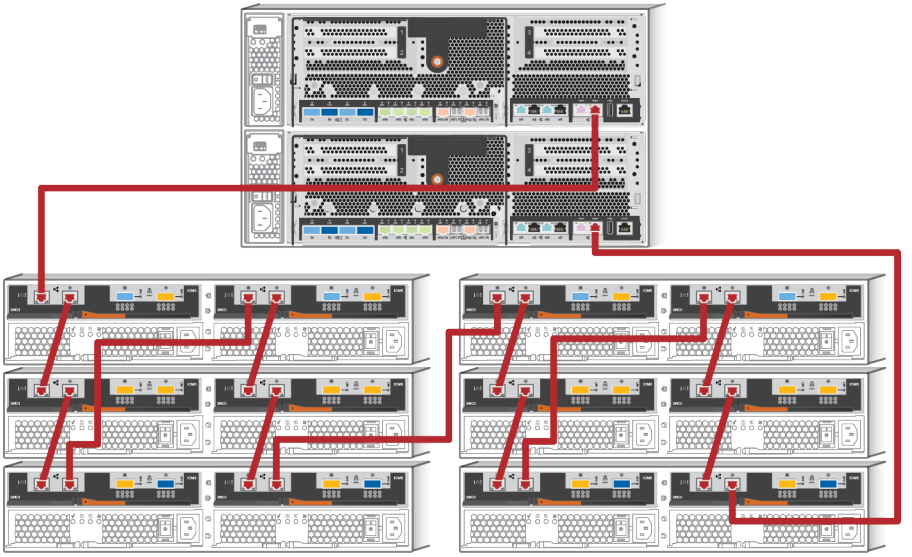
3. Connect the final ACP port with the round symbol to the private management port e0P of controller 2 in the HA pair.
4. Repeat for the other HA pairs in the cluster.

Example

The following diagram displays the ACP cabling for DS424x disk shelves.



The following diagram displays the ACP cabling for DS2246 disk shelves.



Related information

SAS Disk Shelves Universal SAS and ACP Cabling Guide

Cabling the disk shelf SAS data ports

By cabling the serial-attached SCSI (SAS) ports, you can enable each controller in the HA pair to access its own disks and the disks of its partner controller.

Before you begin

You must have located and marked which disk shelves go with each storage controller.

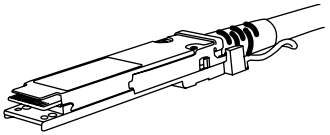
About this task

Disk shelf cabling is always isolated within the HA pair that owns the disks. Disk shelves are never connected to other HA pairs in the cluster.

QSFP to QSFP SAS cables are used to connect disk shelves together and to connect disk shelves to the SAS ports on the controller.

Attention: It is possible to insert the QSFP connector incorrectly (upside down). The connector can slide in and even appear to click into place. However, the latch cannot engage unless the connector is inserted correctly. After inserting the cable, pull on the connector to ensure that it is latched.

For disk shelf I/O modules and controller onboard SAS ports, the cables must be inserted with the bottom of the connector facing down, as shown in the following image. The bottom of the connector is slightly longer than the top, and the latch release is typically on the bottom.



For controller SAS ports on add-in cards, the orientation depends on the slot in which the SAS card is installed. Insert the connector gently, and be sure that it latches securely. If the connector does not latch, rotate it 180 degrees and try again.

These instructions assume two stacks of disk shelves per HA pair. You can split your disk shelves into additional stacks to increase I/O throughput. Additional stacks require adding additional SAS ports to the storage controllers.

SAS ports on both controllers and disk shelves are indicated by the 

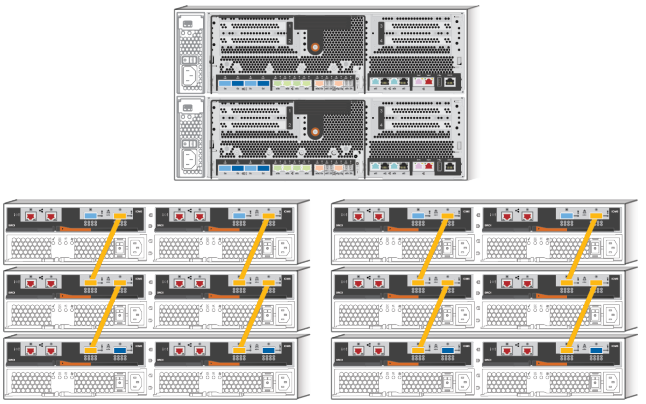
symbol.

Steps

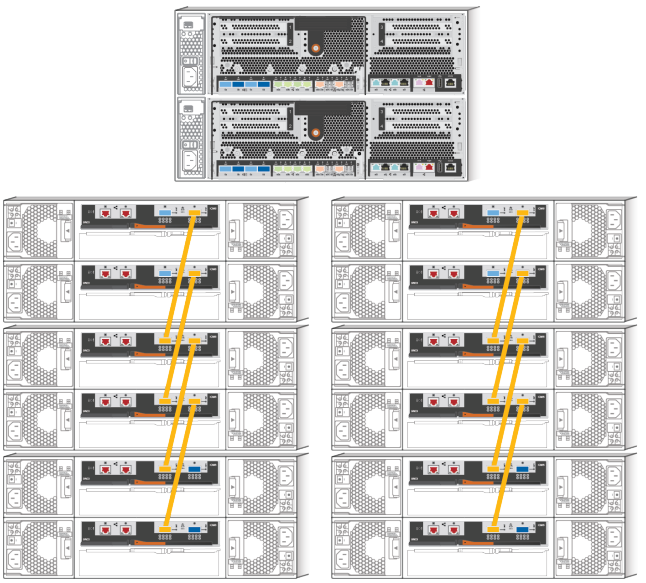
1. Starting with the first stack of disk shelves, cable the I/O modules of the stacks to each other.
   a. Connect the IOM A SAS port with the circle symbol from the first shelf to the IOM A SAS port with the square symbol on the second shelf.
   b. Continue connecting IOM A ports on the remaining disk shelves in the stack, from the ports with a circle symbol to the ports with a square symbol.
   c. Connect the IOM B SAS port with the circle symbol from the first shelf to the IOM B SAS port with the square symbol on the second shelf.
   d. Continue connecting IOM B ports on the remaining disk shelves in the stack, from the ports with a circle symbol to the ports with a square symbol.

   Example

   The following example displays the DS2246 disk shelf cabling:



The following example displays the DS424x disk shelf cabling:



2. Repeat Step 1 for each stack of disk shelves.
3. Connect the first set of controller-to-shelf SAS cables.
   a. Connect the controller 1 SAS port 0a to the SAS port with the square symbol on the first disk shelf in the first stack.
   b. Connect the controller 1 SAS port 0c to the SAS port with the square symbol on the first disk shelf in the second stack.

      This step is not applicable to the FAS8020.

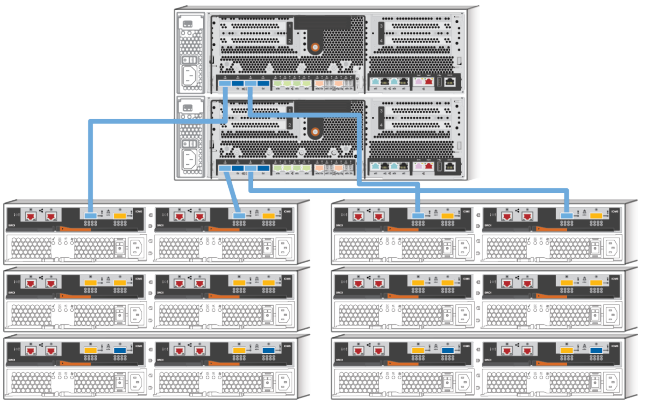
c. Connect the controller 2 SAS port 0a to the SAS port with the square symbol on the second disk shelf in the first stack.

d. Connect the controller 2 SAS port 0c to the SAS port with the square symbol on the second disk shelf in the second stack.

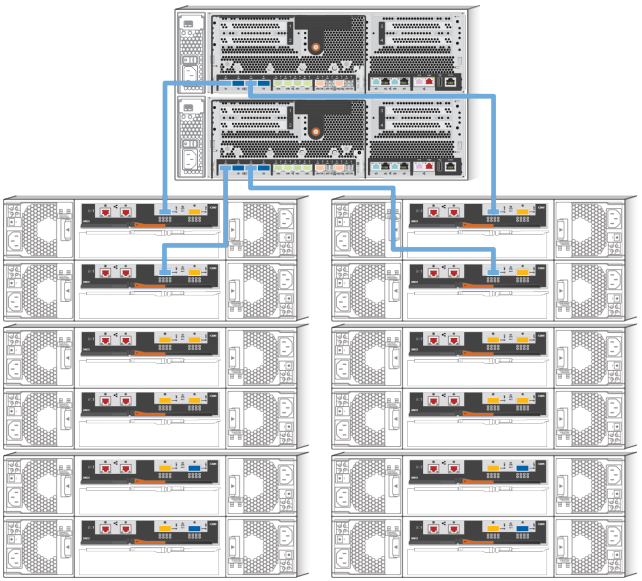
   This step is not applicable to the FAS8020.

Example

The following example displays the first set of controller-to-shelf cabling with DS2246 disk shelves:



The following example displays the first set of controller-to-shelf cabling with DS424x disk shelves:



4. Connect the last set of controller-to-shelf SAS cables.

   a. Connect the controller 1 SAS port 0b to the SAS port with the circle symbol on the last disk shelf in the last stack.

   b. Connect the controller 1 SAS port 0d to the SAS port with the circle symbol on the last disk shelf in the first stack.

      This step is not applicable to the FAS8020.

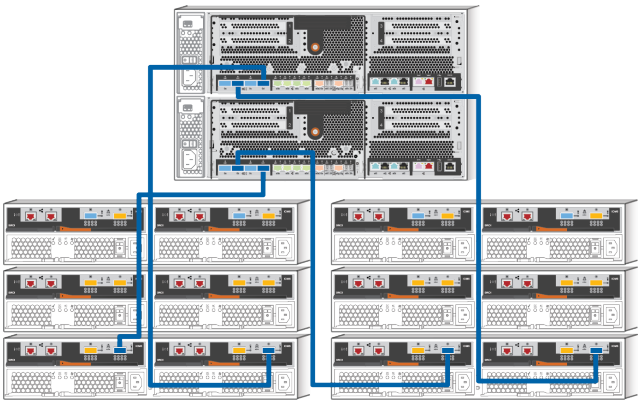
   c. Connect the controller 2 SAS port 0b to the SAS port with the circle symbol on the next-to-last disk shelf in the last stack.

   d. Connect the controller 2 SAS port 0d to the SAS port with the circle symbol on the next-to-last disk shelf in the first stack.

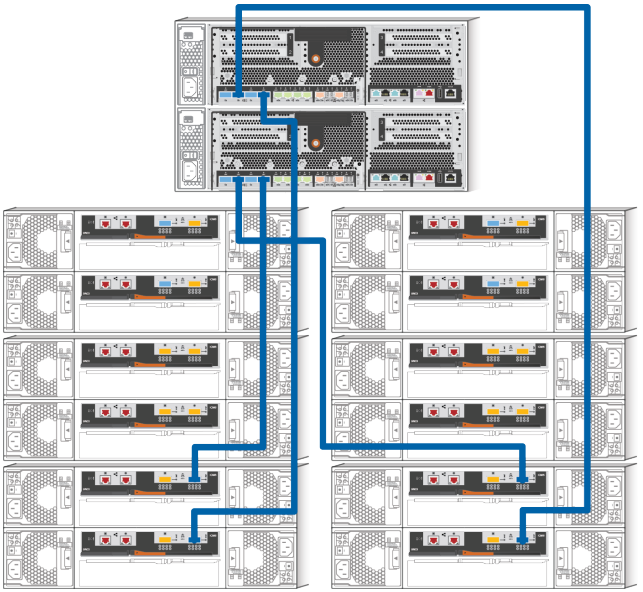
      This step is not applicable to the FAS8020.

Example

The following example displays the last set of controller-to-shelf cabling with DS2246 disk shelves:



The following example displays the last set of controller-to-shelf cabling with DS424x disk shelves:



5. Repeat all steps for the other HA pairs in the cluster.

Related information

SAS Disk Shelves Universal SAS and ACP Cabling Guide

Cabling the HA pair NVRAM ports on storage systems with an I/O expansion module

By cabling the nonvolatile RAM (NVRAM) ports of the two controllers in an HA pair, you enable the pair to mirror its write cache and perform HA monitoring.

About this task

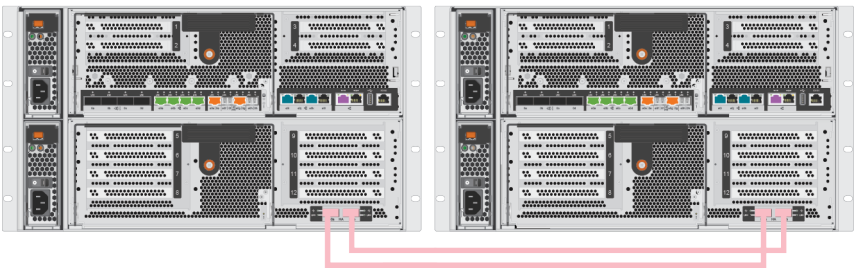
This task does not apply to systems with two controllers in the same chassis; the HA pair connection is made internally through the chassis backplane.

You should use the supplied QSFP+ type copper or optical 40 Gbps Infiniband cables.

Steps

1. Connect port ib0a on the first controller in the HA pair to port ib0a on the other controller.
2. Connect port ib0b on the first controller in the HA pair to port ib0b on the other controller.
3. Repeat for the other HA pairs in the cluster.

Example



Cabling the CN1601 storage controller management ports

Cabling the storage controller management ports enables you to manage the cluster using the CLI or System Manager, after you have set up the cluster using System Setup. The private cluster switch management ports enable you to manage the switches.

About this task

You can connect the controller and cluster switch management ports to existing switches in your network or to new dedicated network switches, such as NetApp CN1601 cluster management switches.

Cabling the management ports also enables System Setup to discover storage controllers when static node-management IP addresses are used.

Steps

1. To cable the node management ports:
   a. Connect the wrench port  of the first storage controller in HA pair to the CN1601 switch.
   b. Connect the wrench port  of the second storage controller in the HA pair to the other CN1601 switch.
   c. Repeat for the other HA pairs in the cluster.
2. To cable the cluster management ports:

If you have a...	Then...
FAS8020 series	**a.** Connect port e0e of the first storage controller to the first CN1601 switch. **b.** Connect port e0f of the first storage controller to the second CN1601 switch. **c.** Connect port e0e of the second storage controller to the first CN1601 switch. **d.** Connect port e0f of the second storage controller to the second CN1601 switch. **e.** Repeat for the other HA pairs in the cluster.
FAS8040, FAS8060, or FAS8080 series	**a.** Connect port e0i of the first storage controller to the first CN1601 switch. **b.** Connect port e0k of the first storage controller to the second CN1601 switch. **c.** Connect port e0i of the second storage controller to the first CN1601 switch. **d.** Connect port e0k of the second storage controller to the second CN1601 switch. **e.** Repeat for the other HA pairs in the cluster.

3. Connect the management port of the first private cluster switch to the CN1601 switch.
4. Connect the management port of the second private cluster switch to the other CN1601 switch.

Cabling the private cluster interconnect for FAS80xx systems

By cabling the private cluster interconnect, you can enable the cluster nodes to communicate with each other, to support data traffic, move volumes, use SnapMirror between clusters, and relocate aggregates.

About this task

The private cluster interconnect uses dedicated 10 GbE ports connected using SFP modules or Twinax, and optionally 10GbE switches for a switched cluster.

For FAS8020 systems, two cluster interconnects per node are required.

For FAS8040, FAS8060, and FAS8080 systems, four cluster interconnects per node are recommended.

You should cable cluster interconnects as pairs. Using an odd number of cluster interconnect connections is not supported.

Steps

1. Cable the private cluster interconnect, depending on your configuration.

If you have a...	Then...
2-node or 4-node switched FAS8020 series	**a.** Connect port e0a of the first storage controller to port 1 of switch 1. **b.** Connect port e0b of the first storage controller to port 1 of switch 2.
2-node or 4-node switched FAS8040, FAS8060, or FAS8080 series	**a.** Connect port e0a of the first storage controller to port 1 of switch 1. **b.** Connect port e0d of the first storage controller to port 2 of switch 1. **c.** Connect port e0c of the first storage controller to port 1 of switch 2. **d.** Connect port e0b of the first storage controller to port 2 of switch 2.
2-node FAS8020 switchless configuration	**a.** Connect port e0a of the first storage controller to port e0a of the second storage controller. **b.** Connect port e0b of the first storage controller to port e0b of the second storage controller.
2-node FAS8040, FAS8060 and FAS8080 switchless configuration	**a.** Connect port e0a of the first storage controller to port e0a of the second storage controller. **b.** Connect port e0c of the first storage controller to port e0c of the second storage controller.

2. Repeat for the other storage controllers in the cluster.

   If you use two connections per controller, connect the second controller to port 2 of each switch, the third controller to port 3, and so on. If you use four connections per controller, connect the second controller to port 3 and 4 of each switch, the third controller to port 5 and 6, and so on.

Related information

NetApp Hardware Universe

Cabling the private cluster ISLs for NetApp CN1610 switches

The four Inter-Switch Links (ISLs) between the two private cluster interconnect switches enable high availability of the cluster network.

About this task

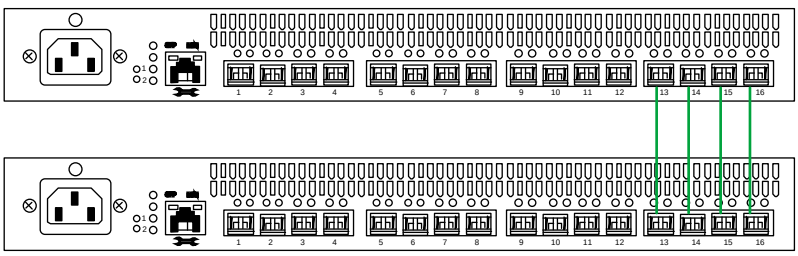
The ISLs use 10 GbE copper cables. The required cables are supplied with the system.

Steps

1. Connect port 13 of the top cluster switch to port 13 of the bottom cluster switch.
2. Repeat for ports 14 through 16.

   There are four ISLs.

NetApp CN1610 cluster switch ISL cabling



Related information

Clustered Data ONTAP 8.3 Network Management Guide

Cabling the Ethernet data networks

Ethernet ports on the storage controllers enable data traffic for NFS and CIFS. In a SAN environment, Ethernet ports also enable iSCSI initiators in your hosts to connect to the iSCSI targets in the storage controller using cables that you supply.

About this task

You must connect to two or more separate networks for high availability. The specific controller ports you use depend on the controller model, bandwidth requirements, and the network speed and media. You can use more ports or faster ports for higher bandwidth.

Onboard UTA2 ports can be configured as either Ethernet or FC. Before cabling, verify that the ports are configured for Ethernet.

Steps

1. Cable one or more Ethernet ports from the first storage controller to an Ethernet switch in your data network.
2. Cable one or more Ethernet ports from the first storage controller to a different Ethernet switch in your data network.
3. Repeat these steps for the other storage controllers in the cluster.
4. Record which storage controller ports connect to which switch ports in your network.

Related information

Clustered Data ONTAP 8.3 Network Management Guide
Clustered Data ONTAP 8.3 SAN Administration Guide

Cabling the Fibre Channel data fabrics

The FC ports on the storage controllers enable FC initiators in your hosts to connect to the FC targets in the storage controller using cables that you supply. You can also use the FC ports to connect to backup devices, such as tape drives.

About this task

You should use two or more separate fabrics for high availability. The specific ports you use depend on the controller model.

FC ports might default to initiator mode. For FC ports used as targets, you can change the port's type and mode from initiator to target after the node is running by using the `system node hardware unified-connect modify` command.

Onboard UTA2 ports can be configured as either Ethernet or FC, but you must use UTA2 ports to use FC. Before cabling, verify that the ports are configured for FC and have the correct SFP+ optical module installed. See the Hardware Universe for information about model numbers for SFP+ optical modules.

Steps

1. Cable one or more FC ports from the first storage controller to an FC switch in your SAN.
2. Cable one or more FC ports from the first storage controller to an FC switch in a different SAN fabric.
3. Repeat these steps for the other storage controllers in the cluster.

Related information

Clustered Data ONTAP 8.3 SAN Configuration Guide
Clustered Data ONTAP 8.3 SAN Administration Guide
NetApp Hardware Universe

Cabling the power supplies

The power supplies provide the electrical power needed to operate the system. The storage components should connect to two independent power sources.

About this task

The supplied cables should fit the power receptacles in typical enclosures for your country. You might need to provide different cables.

All power supplies must be connected to a power source.

Steps

1. Connect the first power supply of each cluster component to the first power source in the enclosure or rack.
2. Connect the second power supply of each cluster component to a second power source in the enclosure or rack.

Powering on switches and disk shelves

You should power on management and cluster switches, and disk shelves before running System Setup. Because System Setup prompts you to turn on your storage controllers, you should not power them on until prompted

Steps

1. Power on the management switches.
2. Power on the cluster switches.

   You can set passwords and configure the switches for alerts after running System Setup.
3. Power on the disk shelves.
4. Inspect the disk shelf IDs to ensure that the factory set IDs are unique to each disk shelf in the storage system.

Completing the System Setup configuration worksheet

The System Setup configuration worksheet enables you to record the values that you need to set up your cluster. If a default value is provided, you should use that value.

About this task

You cannot restart System Setup so it is important to have complete information before beginning.

Step

1. Download and complete the System Setup configuration worksheet.

   Both the worksheet for Data ONTAP 8.2.x and 8.3 are contained in the PDF. You must use the Data ONTAP 8.3 portion of the worksheet.

   System Setup for Clustered Data ONTAP Configuration Worksheet

Downloading and installing System Setup

You must download and install System Setup before you can set up your cluster.

About this task

You cannot restart System Setup so it is important to have complete information before beginning.

You should not power on your storage controllers until prompted by System Setup.

Steps

1. Download System Setup 3.0 or later from the NetApp Support Site.

   NetApp Downloads: System Setup for Windows

2. Install the software on your Windows client.
3. Cable the Windows client to the same management network as your controllers.

Related information

NetApp Support

Setting up the cluster using System Setup

You must use System Setup to perform initial configuration of your cluster, including configuring your admin user authentication, creating cluster and node management interfaces, provisioning disks, creating SVMs, and configuring protocols.

Steps

1. Launch System Setup.
2. Discover the storage controllers.

   System Setup can take up to eight minutes to discover all nodes and configures cluster ports, cluster network interfaces, and validates intra-cluster switch networks and cluster switches.

   If discovery fails, see the System Setup Release Notes.

   Example

3. Create the cluster.
4. Create and configure the management network.

   Node and cluster management interfaces cannot be created on different network subnets.

5. Click **Add Subnet** to create and configure additional data networks, including SVM management and file access, and iSCSI access.

   You must define all IP addresses or address ranges used for this network.

6. Enable AutoSupport.

   HTTPS is the default transport protocol. SMTP is not supported.

7. Configure the storage.

   System Setup cannot provision more than 72 disks.

8. Create the initial data SVM and associated networks.

9. Enable protocols.

   System Setup does not configure FC protocol. If you use FC, you should configure it after completing System Setup tasks.

10. Verify the cluster configuration summary.

Related information

NetApp Documentation: System Setup (current releases)

Configuring CN1610 cluster interconnect switches

You should configure the cluster interconnect switch before use so that the switch can communicate over the management interface. Configuring the cluster interconnect switch includes setting a password, configuring the management network, and enabling the switch to send email alerts if an issue arises.

Steps

1. Log in to the switch as admin and set a password.

   #### Example

   ```
   User:admin
   Password:
   (CN1610) >password
   Enter old password:
   Enter new password:*********
   Confirm new password:*********

   Password Changed!
   ```

2. Configure the switch management port address and hostname.

Example

```
(CN1601) >enable
Password:
(CN1601) #network protocol none
(CN1601) #network parms <<var_mgmt_switch_ IP1>>
<<var_clustermgmt_netmask>> <<var_clustermgmt_gateway>>
(CN1601) #hostname <<var_clustername>>-sw03
```

3. Verify the configuration.

Example

```
(CN1601) #show network
Interface Status.............................. Up
IP Address.................................... 10.x.x.x
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.x.x.x
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... fe80::2a0:98ff:fe4b:
8aa0/64
Burned In MAC Address......................... 00:A0:98:4B:8A:A0
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Configured IPv4 Protocol...................... None
Configured IPv6 Protocol...................... None
IPv6 AutoConfig Mode.......................... Disabled
Management VLAN ID............................ 1
```

4. Configure DNS and network time synchronization.

Example

```
(CN1601) #config
(CN1601) (Config)#ip domain name <<var_global_domain_name>>
(CN1601) (Config)#ip name server <<var_global_nameserver_IP1>>
<<var_global_nameserver_IP2>>
(CN1601) (Config)#sntp client mode unicast
(CN1601) (Config)#sntp server <<var_global_ntp_server_name1>>
(CN1601) (Config)#exit
(CN1601) #show sntp
```

5. Configure email alerts.

Example

```
(CN1610) #config
(CN1610) (Config)#mail-server <<var_mail_hosts_ip>>
(CN1610) (Mail-Server) #exit
(CN1610) (Config)#logging email 3
(CN1610) (Config)#logging email urgent 2
(CN1610) (Config)#logging email message-type both to-addr
<<var_storage_admin_email>>
(CN1610) (Config)#logging email from-addr <<var_storage_admin_email>>
(CN1610) (Config)#logging email message-type both subject "Alert from
<<var_clustername>>-sw01"
(CN1610) (Config)#exit
(CN1610) #show logging email config
(CN1610) #show mail-server all config
```

6. Save the changes.

Example

```
(CN1610) #write memory
(CN1610) #reload
```

7. Repeat steps for the second switch.

Deciding where to send high-severity event notifications

Before you configure high-severity EMS event notifications, you need to decide whether to send the notifications to a email address, a syslog server, or an SNMP traphost.

About this task

If your environment already contains a syslog server for aggregating the logged events from other systems, such as servers and applications, then it is easier to use that syslog server also for high-severity event notifications from storage systems.

If your environment does not already contain a syslog server, then it is easier to use email for high-severity event notifications.

If you already forward event notifications to an SNMP traphost, then you might want to monitor that traphost for high-severity events.

Note: SNMP supports only a small subset of the high-severity events. The Technical Report *NetApp Technical Report 4220: SNMP Support in Data ONTAP 8.2.x and Data ONTAP 8.3.x* contains lists of all default events that are supported by SNMP.

Choices

- If you want the EMS to send high-severity event notifications to an email address, see *Configuring high-severity EMS events to send email notifications* on page 29.
- If you want the EMS to forward high-severity event notifications to a syslog server, see *Configuring high-severity EMS events to forward notifications to a syslog server* on page 30.
- If you want the EMS to forward event notifications to an SNMP traphost, see *Configuring SNMP traphosts to receive event notifications* on page 31

Configuring high-severity EMS events to send email notifications

To receive email notifications of the most severe events, you must configure the EMS to send email messages for the top three severity levels (Critical, Alert, Emergency) and a few additional events that signal high-severity activity.

Before you begin

DNS must be configured on the cluster to resolve the email addresses.

About this task

Before you configure the events, you must first create a dedicated email destination for the event notifications. Event email notifications are sent to configured email addresses using SMTP.

This task configures all events of severity level Critical, Alert, and Emergency. It also configures a selected group of additional events that also report high-severity activity. You must configure all these events to make sure you are notified of system issues that require prompt attention.

You can perform this task any time the cluster is running by entering the commands on the Data ONTAP command line.

Steps

1. Configure the event SMTP mail server settings:

   ```
   event config modify -mailserver mailhost@your_domain
   -mailfrom cluster_name@your_domain
   ```

2. Create an email destination for high-severity event notifications:

   ```
   event destination create -name important_events
   -mail your_email@your_domain
   ```

3. Configure all high-severity events to send email notifications.

   a. Configure all events of severity level Critical, Alert, and Emergency to send email notifications to the email address important_events that you just created:

      ```
      event route add-destinations {-severity CRITICAL|ALERT|EMERGENCY}
      -destinations important_events
      ```

b. Configure additional high-severity events to send email notifications to important_events:

```
event route add-destinations {csm.sessionFailed| secd.dns*| secd.nis*|
secd.ldap*| callhome.aggr.restricted| callhome.c.fan*|
callhome.carrier.fault| callhome.ch.ps.*| callhome.chassis.*|
callhome.client.app.emerg| callhome.client.app.crit|
callhome.client.app.alert| callhome.cpu*| callhome.hm.alert.*|
callhome.netif.fatal.error| callhome.reboot*|
callhome.sblade.import.susp| callhome.sblade.unavailable|
callhome.sfo.giveback| callhome.sfo.takeover*| callhome.shlf.overtemp|
callhome.shlf.power.intr| callhome.spm.process.maxexit|
callhome.clus.vol.cre.fail | clam.takeover |
clam.heartbeat.state.change} -destinations important_events
```

Configuring high-severity EMS events to forward notifications to a syslog server

To log notifications of the most severe events on a syslog server, you must configure the EMS to forward notifications for the top three severity levels (Critical, Alert, Emergency) and a few additional events that signal high-severity activity.

Before you begin

DNS must be configured on the cluster to resolve the syslog server name.

About this task

If your environment does not already contain a syslog server for event notifications, you must first create one. If your environment already contains a syslog server for logging events from other systems, then you might want to use that one for high-severity event notifications.

This task configures all events of severity level Critical, Alert, and Emergency. It also configures a selected group of additional events that also report high-severity activity. You must configure all these events to make sure you are notified of system issues that require prompt attention.

You can perform this task any time the cluster is running by entering the commands on the Data ONTAP command line.

Steps

1. Create a syslog server destination for high-severity events:

   ```
   event destination create -name syslog_ems -syslog ip_address
   -syslog-facility default
   ```

2. Configure all high-severity events to forward notifications to the syslog server.

   a. Configure all events of severity level Critical, Alert, and Emergency to forward notifications to the syslog server that you just created or to your existing syslog server:

```
event route add-destinations {-severity CRITICAL|ALERT|EMERGENCY}
-destinations syslog_ems
```

b. Configure additional high-severity events to forward notifications to the syslog server:

```
event route add-destinations {csm.sessionFailed| secd.dns*| secd.nis*|
secd.ldap*| callhome.aggr.restricted| callhome.c.fan*|
callhome.carrier.fault| callhome.ch.ps.*| callhome.chassis.*|
callhome.client.app.emerg| callhome.client.app.crit|
callhome.client.app.alert| callhome.cpu*| callhome.hm.alert.*|
callhome.netif.fatal.error| callhome.reboot*|
callhome.sblade.import.susp| callhome.sblade.unavailable|
callhome.sfo.giveback| callhome.sfo.takeover*| callhome.shlf.overtemp|
callhome.shlf.power.intr| callhome.spm.process.maxexit|
callhome.clus.vol.cre.fail | clam.takeover |
clam.heartbeat.state.change} -destinations syslog_ems
```

Configuring SNMP traphosts to receive event notifications

To receive event notifications on an SNMP traphost, you must configure a traphost. SNMP supports only a small subset of the top three severity level events (Critical, Alert, Emergency) and none of the additional events that signal high-severity activity.

Before you begin

- SNMP and SNMP traps must be enabled on the cluster.

  Note: SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster to resolve the traphost names.

About this task

If you do not already have an SNMP traphost configured to receive event notifications (SNMP traps), you must add one.

The Technical Report *NetApp Technical Report 4220: SNMP Support in Data ONTAP 8.2.x and Data ONTAP 8.3.x* contains lists of all default events that are supported by SNMP.

You can perform this task any time the cluster is running by entering the commands on the Data ONTAP command line.

Step

1. If your environment does not already have an SNMP traphost configured to receive event notifications, add one:

   ```
   system snmp traphost add -peer-address snmp_traphost_name
   ```

   All event notifications that are supported by SNMP by default are forwarded to the SNMP traphost, which includes both high-severity and low-severity event notifications.

Using Config Advisor to verify cabling

You must download and install Config Advisor so that you can verify that your storage systems are cabled correctly.

Downloading and installing Config Advisor

You must install the Config Advisor tool so that you can verify that your system is cabled correctly.

Before you begin

You must have a laptop that you can connect to the cluster.

About this task

If you need support for the Config Advisor tool, you must follow the procedure in the tool's online Help topic “Reporting issues in Config Advisor.” The Config Advisor tool is not supported by the typical NetApp support process.

Step

1. Download the Config Advisor software and its documentation, and follow the installation instructions in the documentation.

   NetApp Downloads: Config Advisor

Verifying cabling

You can use the Config Advisor tool to verify that the cluster is cabled correctly.

About this task

If you require support for the Config Advisor tool, you must follow the procedure in the tool's online Help topic “Reporting issues in Config Advisor”. The Config Advisor tool is not supported by the typical NetApp support process.

Additional verification of the system is completed as part of the protocol configuration process.

Steps

1. Connect the laptop that contains Config Advisor to the management network for the cluster.
2. Optional: Change the IP address of your laptop to an unused address on the subnet for the management network.
3. Start Config Advisor, and then select the profile **Clustered Data ONTAP**.

4. Select the cluster switch model.
5. Enter the requested IP addresses and credentials.
6. Click **Collect Data**.

   The Config Advisor tool displays any problems found. If problems are found, you must correct them and run the tool again.

Completing protocol configuration and verifying cluster setup

After System Setup enables protocols and creates a Storage Virtual Machine (SVM), you must complete the protocol configuration by using one or more of the protocol Express Guides. System Setup does not support FC, so to configure it and to verify FC cabling, you must use one of the FC Configuration Express Guides.

Step

1. Follow the instructions in one or more of the protocol Express Guides.

   - *Clustered Data ONTAP 8.3 CIFS and NFS Multiprotocol Configuration Express Guide*

     Describes how to quickly configure shared CIFS/SMB and NFSv3 client access to the same files contained in a new volume in either a new SVM or an existing SVM in clustered Data ONTAP 8.3.

   - *Clustered Data ONTAP 8.3 CIFS/SMB Configuration Express Guide*

     Describes how to quickly configure CIFS/SMB client access to files contained in a new volume in either a new SVM or an existing SVM in clustered Data ONTAP 8.3.

   - *Clustered Data ONTAP 8.3 NFS Configuration Express Guide*

     Describes how to quickly configure NFSv3 client access to files contained in a new volume in either a new SVM or an existing SVM in clustered Data ONTAP 8.3.

   - *Clustered Data ONTAP 8.3 iSCSI Configuration for Windows Express Guide*

     Describes how to quickly create a LUN in a Data ONTAP 8.3 cluster and connect it to a host running Windows Server 2008 or Window Server 2012 using iSCSI.

   - *Clustered Data ONTAP 8.3 iSCSI Configuration for ESX Express Guide*

     Describes how to quickly create a LUN in a Data ONTAP 8.3 cluster and connect it to a host running ESX 5.x using iSCSI.

   - *Clustered Data ONTAP 8.3 iSCSI Configuration for Red Hat Linux Express Guide*

     Describes how to quickly set up the iSCSI service on an SVM, provision a LUN, and make the LUN available using an iSCSI initiator on a Red Hat Linux host computer.

   - *Clustered Data ONTAP 8.3 FC Configuration for Windows Express Guide*

Describes how to quickly create a LUN in a Data ONTAP 8.3 cluster and connect it to a host running Windows Server 2008 or Window Server 2012 using FC.

- *Clustered Data ONTAP 8.3 FC Configuration for ESX Express Guide*
  Describes how to quickly create a LUN in a Data ONTAP 8.3 cluster and connect it to a host running ESX 5.x using FC.
- *Clustered Data ONTAP 8.3 FC Configuration for Red Hat Linux Express Guide*
  Describes how to quickly set up the FC service on an SVM, provision a LUN, and make the LUN available using an FC HBA on a Red Hat Linux host computer.

Where to find additional information

After you have finished initial setup, you can continue configuring the cluster using additional resources.

- *NetApp Documentation: Clustered Data ONTAP Express Guides*
  Specific express guides describe how to configure protocols and to verify setup.
- *Clustered Data ONTAP 8.3 Network Management Guide*
  Describes how to configure and manage physical and virtual network ports (VLANs and interface groups), LIFs using IPv4 and IPv6, routing, and host-resolution services in clusters; optimize network traffic by load balancing; and monitor the cluster by using SNMP.
- *Clustered Data ONTAP 8.3 Physical Storage Management Guide*
  Describes how to manage physical storage resources for FlexVol volumes and Infinite Volumes in clusters, including disks, RAID groups, and aggregates.
- *Clustered Data ONTAP 8.3 System Administration Guide for Cluster Administrators*
  Describes general system administration of a cluster, including the CLI interface, cluster access, node management, Storage Virtual Machine (formerly Vserver) setup, user account management, event monitoring, and performance evaluation.
- *Clustered Data ONTAP 8.3 Cluster Management Using OnCommand System Manager*
  This printable version of System Manager online Help describes how to configure, manage, and monitor storage objects and storage systems running clustered Data ONTAP.

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, 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, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at *http://www.netapp.com/us/legal/netapptmlist.aspx*.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

How to send comments about documentation and receive update notification

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

Index

E

F

H

I

L

M

N

P

R

S

T

U

W