Contents

Deciding whether to use this guide ............................................................. 6
Preparing for the MetroCluster installation .............................................. 7
  Differences between the ONTAP MetroCluster configurations ..........  7
  Considerations for configuring cluster peering ..................................... 8
  Prerequisites for cluster peering ............................................................ 8
  Considerations when using dedicated ports ......................................... 9
  Considerations when sharing data ports .............................................. 9
  Considerations when using unmirrored aggregates .......................... 10
  Preconfigured settings for new MetroCluster systems from the factory 10
  Hardware setup checklist ................................................................. 11
Choosing the correct installation procedure for your configuration .... 13
Cabling a two-node SAS-attached stretch MetroCluster configuration .............. 14
  Parts of a two-node SAS-attached stretch MetroCluster configuration 14
  Required MetroCluster hardware components and naming guidelines for two-
  node SAS-attached stretch configurations ....................................... 15
  Installing and cabling MetroCluster components for two-node SAS-attached
  stretch configurations ..................................................................... 16
  Racking the hardware components ................................................... 17
  Cabling the controllers to each other and the storage shelves .......... 17
  Cabling the cluster peering connections ......................................... 18
  Cabling the management and data connections ............................. 19
Cabling a two-node bridge-attached stretch MetroCluster configuration .......... 20
  Parts of a two-node bridge-attached stretch MetroCluster configuration 20
  Required MetroCluster hardware components and naming conventions for two-
  node bridge-attached stretch configurations ................................... 21
  Information gathering worksheet for FC-to-SAS bridges .................. 23
  Installing and cabling MetroCluster components ............................ 24
  Racking the hardware components .................................................. 24
  Cabling the controllers to each other ............................................. 25
  Cabling the cluster peering connections ....................................... 25
  Cabling the management and data connections ............................. 26
  Installing FC-to-SAS bridges and SAS disk shelves ...................... 26
  In-band management of the FC-to-SAS bridges ........................... 27
  Preparing for the installation ....................................................... 27
  Installing the FC-to-SAS bridge and SAS shelves ......................... 29
Configuring the MetroCluster software in ONTAP ................................. 40
  Gathering required information ..................................................... 41
  IP network information worksheet for site A ................................. 41
  IP network information worksheet for site B .................................. 42
Similarities and differences between standard cluster and MetroCluster configurations ...................................................................................................... 44
Restoring system defaults and configuring the HBA type on a previously used controller module ................................................................................................. 45
Configuring FC-VI ports on a X1132A-R6 quad-port card on FAS8020 systems ... 46
Verifying disk assignment in Maintenance mode in a two-node configuration ...... 48
Verifying the HA state of components .................................................................................................................. 49
Setting up ONTAP in a two-node MetroCluster configuration .......................................................... 50
Configuring the clusters into a MetroCluster configuration .......................................................... 52
Peering the clusters .................................................................................................................. 52
Mirroring the root aggregates .................................................................................. 60
Creating a mirrored data aggregate on each node ........................................................................ 60
Creating unmirrored data aggregates .................................................................................. 61
Implementing the MetroCluster configuration .................................................................................. 63
Configuring FC-to-SAS bridges for health monitoring .................................................................. 65
Checking the MetroCluster configuration .................................................................................. 66
Checking for MetroCluster configuration errors with Config Advisor .................................................. 68
Verifying switchover, healing, and switchback .................................................................................. 68
Installing the MetroCluster Tiebreaker software .................................................................................. 68
Protecting configuration backup files ........................................................................ 69
Testing the MetroCluster configuration .................................................................................. 70
Verifying negotiated switchover .................................................................................. 70
Verifying healing and manual switchback .................................................................................. 71
Loss of a single FC-to-SAS bridge .................................................................................. 73
Verifying operation after power line disruption .................................................................................. 74
Verifying operation after loss of a single storage shelf ........................................................................ 75
Connections in a stretch MetroCluster configurations with array LUNs .......................................................... 80
Example of a stretch MetroCluster configuration with array LUNs .................................................. 80
Examples of two-node stretch MetroCluster configurations with disks and array LUNs .......................................................... 80
Example of a stretch MetroCluster configuration with E-Series storage arrays .................................................. 82
Considerations when removing MetroCluster configurations .......................................................... 83
Using the Active IQ Unified Manager and ONTAP System Manager for further configuration and monitoring .......................................................... 84
Synchronizing the system time using NTP .................................................................................. 84
Considerations when using ONTAP in a MetroCluster configuration .......................................................... 85
FlexGroup support in MetroCluster configurations .................................................................................. 85
Job schedules in a MetroCluster configuration .................................................................................. 85
Cluster peering from the MetroCluster site to a third cluster .......................................................... 85
LDAP client configuration replication in a MetroCluster configuration .................................................. 85
Networking and LIF creation guidelines for MetroCluster configurations .................................................. 86
IPspace object replication and subnet configuration requirements .......................................................... 86
Requirements for LIF creation in a MetroCluster configuration .......................................................... 87
Deciding whether to use the Stretch MetroCluster Installation and Configuration Guide

This guide describes how to install and configure the MetroCluster hardware and software components in a stretch configuration (sometimes referred to as a SAS optical MetroCluster configuration).

You should use this guide for planning, installing, and configuring a stretch MetroCluster configuration under the following circumstances:

• You want to understand the architecture of a stretch MetroCluster configuration
• You want to understand the requirements and best practices for configuring a stretch MetroCluster configuration.
• You want to use the command-line interface (CLI), not an automated scripting tool.

You can find other MetroCluster documentation in the following location:

ONTAP 9 Documentation Center
Preparing for the MetroCluster installation

As you prepare for the MetroCluster installation, you should understand the MetroCluster hardware architecture and required components.

Differences between the ONTAP MetroCluster configurations

The various MetroCluster configurations have key differences in the required components.

In all configurations, each of the two MetroCluster sites is configured as an ONTAP cluster. In a two-node MetroCluster configuration, each node is configured as a single-node cluster.

<table>
<thead>
<tr>
<th>Feature</th>
<th>IP configurations</th>
<th>Fabric-attached configurations</th>
<th>Stretch configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Four or eight-node</td>
<td>Two-node</td>
</tr>
<tr>
<td>Number of controllers</td>
<td>Four</td>
<td>Four or eight</td>
<td>Two</td>
</tr>
<tr>
<td>Uses an FC switch storage fabric</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses an IP switch storage fabric</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Uses FC-to-SAS bridges</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses direct-attached SAS storage</td>
<td>Yes (local attached only)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports ADP</td>
<td>Yes (starting in ONTAP 9.4)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports local HA</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Supports automatic switchover</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports unmirrored aggregates</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports array LUNs</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Considerations for configuring cluster peering

Each MetroCluster site is configured as a peer to its partner site. You should be familiar with the prerequisites and guidelines for configuring the peering relationships and when deciding whether to use shared or dedicated ports for those relationships.

Related information

Cluster and SVM peering express configuration

Prerequisites for cluster peering

Before you set up cluster peering, you should confirm that the connectivity, port, IP address, subnet, firewall, and cluster-naming requirements are met.

Connectivity requirements

Every intercluster LIF on the local cluster must be able to communicate with every intercluster LIF on the remote cluster.

Although it is not required, it is typically simpler to configure the IP addresses used for intercluster LIFs in the same subnet. The IP addresses can reside in the same subnet as data LIFs, or in a different subnet. The subnet belong to the broadcast domain that contains the ports that used for intercluster communication.

Intercluster LIFs can have an IPv4 address or an IPv6 address.

Port requirements

You can use dedicated ports for intercluster communication, or share ports used by the data network. Ports must meet the following requirements:

- All ports that are used to communicate with a given remote cluster must be in the same IPspace. You can use multiple IPspaces to peer with multiple clusters. Pair-wise full-mesh connectivity is required only within an IPspace.
- The broadcast domain that is used for intercluster communication must include at least two ports per node so that intercluster communication can fail over from one port to another port. Ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).
- All ports must be cabled.
- All ports must be in a healthy state.
- The MTU settings of the ports must be consistent.

Firewall requirements

Firewalls and the intercluster firewall policy must allow the following protocols:

- ICMP service
- TCP to the IP addresses of all the intercluster LIFs over the ports 10000, 11104, and 11105
- HTTPS

The default intercluster firewall policy allows access through the HTTPS protocol and from all IP addresses (0.0.0.0/0). You can modify or replace the policy if necessary.
Considerations when using dedicated ports

When determining whether using a dedicated port for intercluster replication is the correct intercluster network solution, you should consider configurations and requirements such as LAN type, available WAN bandwidth, replication interval, change rate, and number of ports.

Consider the following aspects of your network to determine whether using a dedicated port is the best intercluster network solution:

- If the amount of available WAN bandwidth is similar to that of the LAN ports and the replication interval is such that replication occurs while regular client activity exists, then you should dedicate Ethernet ports for intercluster replication to avoid contention between replication and the data protocols.

- If the network utilization generated by the data protocols (CIFS, NFS, and iSCSI) is such that the network utilization is above 50 percent, then you should dedicate ports for replication to allow for nondegraded performance if a node failover occurs.

- When physical 10 GbE or faster ports are used for data and replication, you can create VLAN ports for replication and dedicate the logical ports for intercluster replication. The bandwidth of the port is shared between all VLANs and the base port.

- Consider the data change rate and replication interval and whether the amount of data that must be replicated on each interval requires enough bandwidth that it might cause contention with data protocols if sharing data ports.

Considerations when sharing data ports

When determining whether sharing a data port for intercluster replication is the correct intercluster network solution, you should consider configurations and requirements such as LAN type, available WAN bandwidth, replication interval, change rate, and number of ports.

Consider the following aspects of your network to determine whether sharing data ports is the best intercluster connectivity solution:

- For a high-speed network, such as a 40-Gigabit Ethernet (40-GbE) network, a sufficient amount of local LAN bandwidth might be available to perform replication on the same 40-GbE ports that are used for data access. In many cases, the available WAN bandwidth is far less than 10 GbE LAN bandwidth.

- All nodes in the cluster might have to replicate data and share the available WAN bandwidth, making data port sharing more acceptable.

- Sharing ports for data and replication eliminates the extra port counts required to dedicate ports for replication.

- The maximum transmission unit (MTU) size of the replication network will be the same size as that used on the data network.

- Consider the data change rate and replication interval and whether the amount of data that must be replicated on each interval requires enough bandwidth that it might cause contention with data protocols if sharing data ports.

- When data ports for intercluster replication are shared, the intercluster LIFs can be migrated to any other intercluster-capable port on the same node to control the specific data port that is used for replication.
Considerations when using unmirrored aggregates

If your configuration includes unmirrored aggregates, you must be aware of potential access issues after switchover operations.

Considerations for unmirrored aggregates when doing maintenance requiring power shutdown

If you are performing negotiated switchover for maintenance reasons requiring site-wide power shutdown, you should first manually take offline any unmirrored aggregates owned by the disaster site.

If you do not, nodes at the surviving site might go down due to multi-disk panics. This could occur if switched-over unmirrored aggregates go offline or are missing because of the loss of connectivity to storage at the disaster site due to the power shutdown or a loss of ISLs.

Considerations for unmirrored aggregates and hierarchical namespaces

If you using hierarchical namespaces, you should configure the junction path so that all of the volumes in that path are either on mirrored aggregates only or on unmirrored aggregates only. Configuring a mix of unmirrored and mirrored aggregates in the junction path might prevent access to the unmirrored aggregates after the switchover operation.

Considerations for unmirrored aggregates and CRS MDV and data SVM's root volumes

The configuration replication service (CRS) metadata volume and data SVM's root volumes must be on a mirrored aggregate. You cannot move these volumes to unmirrored aggregate. If they are on unmirrored aggregate, negotiated switchover and switchback operations are vetoed. The metrocluster check command provides a warning if this is the case.

Considerations for unmirrored aggregates and SVMs using SAN protocols

SVMs configured for SAN protocols should be configured on mirrored aggregates only or on unmirrored aggregates only. Configuring a mix of unmirrored and mirrored aggregates can result in a switchover operation that exceeds 120 seconds and result in a data outage if the unmirrored aggregates do not come online.

Preconfigured settings for new MetroCluster systems from the factory

New MetroCluster nodes and, if present, FC-to-SAS bridges are preconfigured and MetroCluster settings are enabled in the software. In most cases, you do not need to perform the detailed procedures provided in this guide.

Hardware racking and cabling

Depending on the configuration you ordered, you might need to rack the systems and complete the cabling.

Cabling a two-node SAS-attached stretch MetroCluster configuration on page 14
Cabling a two-node bridge-attached stretch MetroCluster configuration on page 20
FC-to-SAS bridge configurations

For configurations using FC-to-SAS bridges, the bridges received with the new MetroCluster configuration are preconfigured and do not require additional configuration unless you want to change the names and IP addresses.

Software configuration of the MetroCluster configuration

Nodes received with the new MetroCluster configuration are preconfigured with a single root aggregate. Additional configuration must be performed using the detailed procedures provided in this guide.

Hardware setup checklist

You need to know which hardware setup steps were completed at the factory and which steps you need to complete at each MetroCluster site.

<table>
<thead>
<tr>
<th>Step</th>
<th>Completed at factory</th>
<th>Completed by you</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mount components in one or more cabinets.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Position cabinets in the desired location.</td>
<td>No</td>
<td>Yes Position them in the original order so that the supplied cables are long enough.</td>
</tr>
<tr>
<td>Connect multiple cabinets to each other, if applicable.</td>
<td>No</td>
<td>Yes Use the cabinet interconnect kit if it is included in the order. The kit box is labeled.</td>
</tr>
<tr>
<td>Secure the cabinets to the floor, if applicable.</td>
<td>No</td>
<td>Yes Use the universal bolt-down kit if it is included in the order. The kit box is labeled.</td>
</tr>
<tr>
<td>Cable the components within the cabinet.</td>
<td>Yes Cables 5 meters and longer are removed for shipping and placed in the accessories box.</td>
<td>No</td>
</tr>
<tr>
<td>Connect the cables between cabinets, if applicable.</td>
<td>No</td>
<td>Yes Cables are in the accessories box.</td>
</tr>
<tr>
<td>Step</td>
<td>Completed at factory</td>
<td>Completed by you</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Connect management cables to the customer's network.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Connect console ports to the customer's terminal server, if applicable.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Connect the customer's data cables to the cluster.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Connect the cabinets to power and power on the components.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Verify cabling by running the Config Advisor tool.</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Attention: To avoid address conflicts, do not connect management ports to the customer's network until after you change the default IP addresses to the customer's values.

Power them on in the following order:
1. PDUs
2. Disk shelves and FC-to-SAS bridges, if applicable
3. Nodes
Choosing the correct installation procedure for your configuration

You must choose the correct installation procedure based on whether you are using FlexArray LUNs and how the storage controllers connect to the storage shelves.

<table>
<thead>
<tr>
<th>For this installation type...</th>
<th>Use these procedures...</th>
</tr>
</thead>
</table>
| Two-node stretch configuration with FC-to SAS bridges | 1. *Cabling a two-node bridge-attached stretch MetroCluster configuration* on page 20  
2. *Configuring the MetroCluster software in ONTAP* on page 40 |
| Two-node stretch configuration with direct-attached SAS cabling | 1. *Cabling a two-node SAS-attached stretch MetroCluster configuration* on page 14  
2. *Configuring the MetroCluster software in ONTAP* on page 40 |
| Installation with array LUNs | *Connections in a stretch MetroCluster configurations with array LUNs* on page 80 |
Cabling a two-node SAS-attached stretch MetroCluster configuration

The MetroCluster components must be physically installed, cabled, and configured at both geographic sites. The steps are slightly different for a system with native disk shelves as opposed to a system with array LUNs.

About this task

Parts of a two-node SAS-attached stretch MetroCluster configuration

The two-node MetroCluster SAS-attached configuration requires a number of parts, including two single-node clusters in which the storage controllers are directly connected to the storage using SAS cables.

The MetroCluster configuration includes the following key hardware elements:

- **Storage controllers**
  The storage controllers connect directly to the storage using SAS cables.
  Each storage controller is configured as a DR partner to a storage controller on the partner site.
  - Copper SAS cables can be used for shorter distances.
  - Optical SAS cables can be used for longer distances.
  
  **Note:** In systems using E-Series array LUNs, the storage controllers can be directly connected to the E-Series storage arrays. For other array LUNs, connections via FC switches are required.

**NetApp Interoperability Matrix Tool**

In the IMT, you can use the Storage Solution field to select your MetroCluster solution. You use the Component Explorer to select the components and ONTAP version to refine your search. You can click Show Results to display the list of supported configurations that match the criteria.

- **Cluster peering network**
  The cluster peering network provides connectivity for mirroring of the storage virtual machine (SVM) configuration. The configuration of all SVMs on one cluster is mirrored to the partner cluster.
Required MetroCluster hardware components and naming guidelines for two-node SAS-attached stretch configurations

The MetroCluster configuration requires a variety of hardware components. For convenience and clarity, standard names for components are used throughout the MetroCluster documentation. Also, one site is referred to as Site A and the other site is referred to as Site B.

Supported software and hardware

The hardware and software must be supported for the MetroCluster FC configuration.

*NetApp Hardware Universe*

When using AFF systems, all controller modules in the MetroCluster configuration must be configured as AFF systems.

Hardware redundancy in the MetroCluster configuration

Because of the hardware redundancy in the MetroCluster configuration, there are two of each component at each site. The sites are arbitrarily assigned the letters A and B and the individual components are arbitrarily assigned the numbers 1 and 2.

Two single-node ONTAP clusters

The SAS-attached stretch MetroCluster configuration requires two single-node ONTAP clusters. Naming must be unique within the MetroCluster configuration.

Example names:

- Site A: cluster_A
- Site B: cluster_B

Two storage controller modules

The SAS-attached stretch MetroCluster configuration requires two storage controller modules.

- Naming must be unique within the MetroCluster configuration.
- All controller modules in the MetroCluster configuration must be running the same version of ONTAP.
- All controller modules in a DR group must be of the same model.
- All controller modules in a DR group must use the same FC-VI configuration.

Some controller modules support two options for FC-VI connectivity:

- Onboard FC-VI ports
- An FC-VI card in slot 1

A mix of one controller module using onboard FC-VI ports and another using an add-on FC-VI card is not supported. For example, if one node uses onboard FC-VI configuration, then all other nodes in the DR group must use onboard FC-VI configuration as well.

Example names:

- Site A: controller_A_1
At least four SAS disk shelves (recommended)

The SAS-attached stretch MetroCluster configuration requires at least two SAS disk shelves. Four SAS disk shelves is recommended.

Two shelves are recommended at each site to allow disk ownership on a per-shelf basis. A minimum of one shelf at each site is supported.

Example names:

- Site A:
  - shelf_A_1_1
  - shelf_A_1_2
- Site B:
  - shelf_B_1_1
  - shelf_B_1_2

Installing and cabling MetroCluster components for two-node SAS-attached stretch configurations

The storage controllers must be cabled to the storage and to each other. The storage controllers must also be cabled to the data and management network.

Before you begin any procedure in this document

The following overall requirements must be met before completing this task:

- You must have familiarized yourself with the considerations and best practices for installing and cabling disk shelves for your disk shelf model.
  NetApp Documentation: Disk Shelves
- All components must be supported.
  NetApp Interoperability Matrix Tool
  In the IMT, you can use the Storage Solution field to select your MetroCluster solution. You use the Component Explorer to select the components and ONTAP version to refine your search. You can click Show Results to display the list of supported configurations that match the criteria.

About this task

- The terms node and controller are used interchangeably.

Choices

- Racking the hardware components on page 17
- Cabling the controllers to each other and the storage shelves on page 17
- Cabling the cluster peering connections on page 18
- Cabling the management and data connections on page 19
Racking the hardware components

If you have not received the equipment already installed in cabinets, you must rack the components.

About this task
This task must be performed on both MetroCluster sites.

Steps
1. Plan the positioning of the MetroCluster components.
   The amount of rack space needed depends on the platform model of the storage controllers, the switch types, and the number of disk shelf stacks in your configuration.
2. Properly ground yourself.
3. Install the storage controllers in the rack or cabinet.

   AFF and FAS Documentation Center
4. Install the disk shelves, daisy-chain the disk shelves in each stack, power them on, and set the shelf IDs.
   See the appropriate guide for your disk shelf model for information about daisy-chaining disk shelves and setting shelf IDs.
   Note: Shelf IDs must be unique for each SAS disk shelf within the entire MetroCluster configuration (including both sites). When manually setting shelf IDs, you must power-cycle the disk shelf.

   NetApp Documentation: Disk Shelves

Cabling the controllers to each other and the storage shelves

The controller FC-VI adapters must be cabled directly to each other. The controller SAS ports must be cabled to both the remote and local storage stacks.

About this task
This task must be performed on both MetroCluster sites.

Steps
1. Cable the FC-VI ports.

   ![Diagram of FC-VI ports](image)

   The above illustration is representative. The specific FC-VI ports vary by controller module.
   - FAS8200 and AFF A300 controller modules can be ordered with one of two options for FC-VI connectivity:
     - Onboard ports 0e and 0f configured in FC-VI mode.
1. Port 1a and 1b on an FC-VI card in slot 1.

2. AFF A700 and FAS9000 storage systems controller modules use four FC-VI ports each.

2. Cable the SAS ports.

See the appropriate guide for your disk shelf model for controller-to-stack cabling rules, worksheets, and examples.

**Note:** You can determine the controller port pairs to cable for your configuration by using the cabling worksheet.

*NetApp Documentation: Disk Shelves*

The following illustration shows the connections. Your port usage might be different, depending on the available SAS and FC-VI ports on the controller module.

---

**Cabling the cluster peering connections**

You must cable the controller module ports used for cluster peering so that they have connectivity with the cluster on the partner site.

**About this task**

This task must be performed on each controller module in the MetroCluster configuration.

At least two ports on each controller module should be used for cluster peering.

The recommended minimum bandwidth for the ports and network connectivity is 1 GbE.

**Step**

1. Identify and cable at least two ports for cluster peering and verify they have network connectivity with the partner cluster.

Cluster peering can be done on dedicated ports or on data ports. Using dedicated ports provides higher throughput for the cluster peering traffic.

*Cluster and SVM peering express configuration*
Cabling the management and data connections

You must cable the management and data ports on each storage controller to the site networks.

About this task

This task must be repeated for each new controller at both MetroCluster sites.

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.

Step

1. Cable the controller's management and data ports to the management and data networks at the local site.

AFF and FAS Documentation Center
Cabling a two-node bridge-attached stretch MetroCluster configuration

The MetroCluster components must be physically installed, cabled, and configured at both geographic sites. The steps are slightly different for a system with native disk shelves as opposed to a system with array LUNs.

About this task

Parts of a two-node bridge-attached stretch MetroCluster configuration

As you plan your MetroCluster configuration, you should understand the parts of the configuration and how they work together.

The MetroCluster configuration includes the following key hardware elements:

- **Storage controllers**
  The storage controllers are not connected directly to the storage but connected to FC-to-SAS bridges. The storage controllers are connected to each other by FC cables between each controller's FC-VI adapters.
  Each storage controller is configured as a DR partner to a storage controller on the partner site.

- **FC-to-SAS bridges**
  The FC-to-SAS bridges connect the SAS storage stacks to the FC initiator ports on the controllers, providing bridging between the two protocols.

- **Cluster peering network**
  The cluster peering network provides connectivity for mirroring of the storage virtual machine (SVM) configuration. The configuration of all SVMs on one cluster is mirrored to the partner cluster.
The following illustration shows a simplified view of the MetroCluster configuration. For some connections, a single line represents multiple, redundant connections between the components. Data and management network connections are not shown.

- The configuration consists of two single-node clusters.
- Each site has one or more stacks of SAS storage.
  
  **Note:** SAS shelves in MetroCluster configurations are not supported with ACP cabling. Additional storage stacks are supported, but only one is shown at each site.

### Required MetroCluster hardware components and naming conventions for two-node bridge-attached stretch configurations

When planning your MetroCluster configuration, you must understand the required and supported hardware and software components. For convenience and clarity, you should also understand the naming conventions used for components in examples throughout the documentation. For example, one site is referred to as Site A and the other site is referred to as Site B.

#### Supported software and hardware

The hardware and software must be supported for the MetroCluster FC configuration.

**NetApp Hardware Universe**

When using AFF systems, all controller modules in the MetroCluster configuration must be configured as AFF systems.

#### Hardware redundancy in the MetroCluster configuration

Because of the hardware redundancy in the MetroCluster configuration, there are two of each component at each site. The sites are arbitrarily assigned the letters A and B and the individual components are arbitrarily assigned the numbers 1 and 2.

#### Requirement for two single-node ONTAP clusters

The bridge-attached stretch MetroCluster configuration requires two single-node ONTAP clusters. Naming must be unique within the MetroCluster configuration.
Example names:

- Site A: cluster_A
- Site B: cluster_B

**Requirement for two storage controller modules**

The bridge-attached stretch MetroCluster configuration requires two storage controller modules. The controllers must meet the following requirements:

- Naming must be unique within the MetroCluster configuration.
- All controller modules in the MetroCluster configuration must be running the same version of ONTAP.
- All controller modules in a DR group must be of the same model.
- All controller modules in a DR group must use the same FC-VI configuration.
  Some controller modules support two options for FC-VI connectivity:
  - Onboard FC-VI ports
  - An FC-VI card in slot 1

A mix of one controller module using onboard FC-VI ports and another using an add-on FC-VI card is not supported. For example, if one node uses onboard FC-VI configuration, then all other nodes in the DR group must use onboard FC-VI configuration as well.

Example names:

- Site A: controller_A_1
- Site B: controller_B_1

**Requirement for FC-to-SAS bridges**

The bridge-attached stretch MetroCluster configuration requires two or more FC-to-SAS bridges at each site.

These bridges connect the SAS disk shelves to the controller modules.

- FibreBridge 7600N and 7500N bridges support up to four SAS stacks.
- FibreBridge 6500N bridges support only one SAS stack.
- Each stack can use different models of IOM, but all shelves within a stack must use the same model.
  The supported IOM models depend on the ONTAP version you are running.
- Naming must be unique within the MetroCluster configuration.

The suggested names used as examples in this guide identify the controller module that the bridge connects to and the port.

Example names:

- Site A:
  - bridge_A_1_port-number
  - bridge_A_2_port-number
- Site B:
Requirement for at least four SAS shelves (recommended)

The bridge-attached stretch MetroCluster configuration requires at least two SAS shelves. However, two shelves are recommended at each site to allow disk ownership on a per-shelf basis, for a total of four SAS shelves.

A minimum of one shelf at each site is supported.

Example names:

- Site A:
  - shelf_A_1_1
  - shelf_A_1_2
- Site B:
  - shelf_B_1_1
  - shelf_B_1_2

Information gathering worksheet for FC-to-SAS bridges

Before beginning to configure the MetroCluster sites, you should gather required configuration information.

Site A, FC-to-SAS bridge 1 (FC_bridge_A_1a)

Each SAS stack requires at least two FC-to-SAS bridges.

Each bridge connects to Controller_A_1_port-number and Controller_B_1_port-number.

<table>
<thead>
<tr>
<th>Site A</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_A_1a IP address</td>
<td></td>
</tr>
<tr>
<td>Bridge_A_1a Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_A_1a Password</td>
<td></td>
</tr>
</tbody>
</table>

Site A, FC-to-SAS bridge 2 (FC_bridge_A_1b)

Each SAS stack requires at least two FC-to-SAS bridges.

Each bridge connects to Controller_A_1_port-number and Controller_B_1_port-number.

<table>
<thead>
<tr>
<th>Site A</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_A_1b IP address</td>
<td></td>
</tr>
<tr>
<td>Bridge_A_1b Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_A_1b Password</td>
<td></td>
</tr>
</tbody>
</table>

Site B, FC-to-SAS bridge 1 (FC_bridge_B_1a)

Each SAS stack requires at least two FC-to-SAS bridges.

Each bridge connects to Controller_A_1_port-number and Controller_B_1_port-number.
Site B

<table>
<thead>
<tr>
<th>Bridge_B_1a IP address</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_B_1a Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_1a Password</td>
<td></td>
</tr>
</tbody>
</table>

Site B, FC-to-SAS bridge 2 (FC_bridge_B_1b)

Each SAS stack requires at least two FC-to-SAS bridges.

Each bridge connects to Controller_A_1_port-number and Controller_B_1_port-number.

<table>
<thead>
<tr>
<th>Bridge_B_1b IP address</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge_B_1b Username</td>
<td></td>
</tr>
<tr>
<td>Bridge_B_1b Password</td>
<td></td>
</tr>
</tbody>
</table>

Installing and cabling MetroCluster components

The storage controllers must be cabled to the storage and to each other. The storage controllers must also be cabled to the data and management networks.

Steps
1. Racking the hardware components on page 24
2. Cabling the controllers to each other on page 25
3. Cabling the cluster peering connections on page 25
4. Cabling the management and data connections on page 26

Racking the hardware components

If you have not received the equipment already installed in cabinets, you must rack the components.

About this task

This task must be performed on both MetroCluster sites.

Steps
1. Plan out the positioning of the MetroCluster components.
   The rack space depends on the platform model of the storage controllers, the switch types, and the number of disk shelf stacks in your configuration.
2. Properly ground yourself.
3. Install the storage controllers in the rack or cabinet.
   AFF and FAS Documentation Center
4. Install the disk shelves, power them on, and set the shelf IDs.
   NetApp Documentation: Disk Shelves
   - You must power-cycle each disk shelf.
• Shelf IDs must be unique for each SAS disk shelf within the entire MetroCluster configuration (including both sites).

5. Install each FC-to-SAS bridge:
   a. Secure the “L” brackets on the front of the bridge to the front of the rack (flush-mount) with the four screws.
      The openings in the bridge “L” brackets are compliant with rack standard ETA-310-X for 19-inch (482.6 mm) racks.
      For more information and an illustration of the installation, see the ATTO FibreBridge Installation and Operation Manual for your bridge model.
   b. Connect each bridge to a power source that provides a proper ground.
   c. Power on each bridge.
      Note: For maximum resiliency, bridges that are attached to the same stack of disk shelves must be connected to different power sources.
      The bridge Ready LED might take up to 30 seconds to illuminate, indicating that the bridge has completed its power-on self test sequence.

Cabling the controllers to each other

Each controller’s FC-VI adapters must be cabled directly to its partner.

Step

1. Cable the FC-VI ports.

   The above illustration is representative. The specific FC-VI ports vary by controller module.

   • AFF A300 and FAS8200 controller modules can be ordered with one of two options for FC-VI connectivity:
     ◦ Onboard ports 0e and 0f configured in FC-VI mode.
     ◦ Ports 1a and 1b on an FC-VI card in slot 1.
   
   • AFF A700 and FAS9000 storage systems controller modules use four FC-VI ports each.

Cabling the cluster peering connections

You must cable the controller module ports used for cluster peering so that they have connectivity with the cluster on the partner site.

About this task

This task must be performed on each controller module in the MetroCluster configuration.
At least two ports on each controller module should be used for cluster peering.
The recommended minimum bandwidth for the ports and network connectivity is 1 GbE.
Step 1. Identify and cable at least two ports for cluster peering and verify they have network connectivity with the partner cluster.

Cluster peering can be done on dedicated ports or on data ports. Using dedicated ports provides higher throughput for the cluster peering traffic.

Cluster and SVM peering express configuration

Cabling the management and data connections

You must cable the management and data ports on each storage controller to the site networks.

About this task

This task must be repeated for each new controller at both MetroCluster sites.

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.

Step 1. Cable the controller's management and data ports to the management and data networks at the local site.

Installing FC-to-SAS bridges and SAS disk shelves

You install and cable ATTO FibreBridge bridges and SAS disk shelves when adding new storage to the configuration.

About this task

For systems received from the factory, the FC-to-SAS bridges are preconfigured and do not require additional configuration.

This procedure is written with the assumption that you are using the recommended bridge management interfaces: the ATTO ExpressNAV GUI and ATTO QuickNAV utility.

You use the ATTO ExpressNAV GUI to configure and manage a bridge, and to update the bridge firmware. You use the ATTO QuickNAV utility to configure the bridge Ethernet management 1 port.

You can use other management interfaces instead, if needed, such as a serial port or Telnet to configure and manage a bridge and to configure the Ethernet management 1 port, and FTP to update the bridge firmware.

This procedure uses the following workflow:
Steps
1. In-band management of the FC-to-SAS bridges on page 27
2. Preparing for the installation on page 27
3. Installing the FC-to-SAS bridge and SAS shelves on page 29

In-band management of the FC-to-SAS bridges

Beginning with ONTAP 9.5 with FibreBridge 7500N or 7600N bridges, in-band management of the bridges is supported as an alternative to IP management of the bridges.

When using in-band management, the bridges can be managed and monitored from the ONTAP CLI via the FC connection to the bridge. Physical access to the bridge via the bridge Ethernet ports is not required, reducing the security vulnerability of the bridge.

Bridge CLI commands can be issued from the ONTAP interface `storage bridge run-cli -name bridge-name -command bridge-command-name` command at the ONTAP interface.

Note: Using in-band management with IP access disabled is recommended to improve security by limiting physical connectivity the bridge.

Preparing for the installation

When you are preparing to install the bridges as part of your new MetroCluster system, you must ensure that your system meets certain requirements, including meeting setup and configuration.
requirements for the bridges. Other requirements include downloading the necessary documents, the ATTO QuickNAV utility, and the bridge firmware.

**Before you begin**

- Your system must already be installed in a rack if it was not shipped in a system cabinet.
- Your configuration must be using supported hardware models and software versions.
  
  **NetApp Interoperability Matrix Tool**
  
  In the IMT, you can use the Storage Solution field to select your MetroCluster solution. You use the **Component Explorer** to select the components and ONTAP version to refine your search. You can click **Show Results** to display the list of supported configurations that match the criteria.

- Each FC switch must have one FC port available for one bridge to connect to it.
- You must have familiarized yourself with how to handle SAS cables and the considerations and best practices for installing and cabling disk shelves.
  
  The **Installation and Service Guide** for your disk shelf model describes the considerations and best practices.

  **NetApp Documentation: Disk Shelves**

- The computer you are using to set up the bridges must be running an ATTO-supported web browser to use the ATTO ExpressNAV GUI.
  
  The **ATTO Product Release Notes** have an up-to-date list of supported web browsers. You can access this document from the ATTO web site as described in the following steps.

**Steps**

1. Download the *Installation and Service Guide* for your disk shelf model:

   **NetApp Documentation: Disk Shelves**

2. Access the ATTO web site using the link provided for your FibreBridge model and download the manual and the QuickNAV utility.

   **Note:** The *ATTO FibreBridge Installation and Operation Manual* for your model bridge has more information about management interfaces.

   You can access this and other content on the ATTO web site by using the link provided on the ATTO Fibrebridge Description page.

   **NetApp Downloads: ATTO FibreBridge 7600N**

   **NetApp Downloads: ATTO FibreBridge 7500N**

   **NetApp Downloads: ATTO FibreBridge 6500N**

3. Gather the hardware and information needed to use the recommended bridge management interfaces, the ATTO ExpressNAV GUI, and the ATTO QuickNAV utility:

   a. Determine a non-default user name and password (for accessing the bridges).
      
      You should change the default user name and password.

   b. If configuring for IP management of the bridges, you need the shielded Ethernet cable provided with the bridges (which connects from the bridge Ethernet management 1 port to your network).

   c. If configuring for IP management of the bridges, you need an IP address, subnet mask, and gateway information for the Ethernet management 1 port on each bridge.

   d. Disable VPN clients on the computer you are using for setup.
      
      Active VPN clients cause the QuickNAV scan for bridges to fail.
Installing the FC-to-SAS bridge and SAS shelves

After ensuring that the system meets all of the requirements in the “Preparing for the installation” section, you can install your new system.

About this task

• The disk and shelf configuration at both sites should be identical.
  If a non-mirrored aggregate is used, the disk and shelf configuration at each site might be different.
  
  **Note:** All disks in the disaster recovery group must use the same type of connection and be visible to all of the nodes within the disaster recovery group, regardless of the disks being used for mirrored or non-mirrored aggregate.

• The system connectivity requirements for maximum distances for disk shelves, FC switches, and backup tape devices using 50-micron, multimode fiber-optic cables, also apply to FibreBridge bridges.

  **NetApp Hardware Universe**

• A mix of IOM12 modules and IOM6/IOM3 modules is not supported within the same storage stack.

  **Note:** In-band ACP is supported without additional cabling in the following shelves and FibreBridge 7500N or 7600N bridge:

  • IOM12 (DS460C) behind a 7500N or 7600N bridge with ONTAP 9.2 and later
  • IOM12 (DS212C and DS224C) behind a 7500N or 7600N bridge with ONTAP 9.1 and later

  **Note:** SAS shelves in MetroCluster configurations do not support ACP cabling.

Steps

1. Enabling IP port access on the FibreBridge 7600N bridge if necessary on page 29
2. Configuring the FC-to-SAS bridges on page 30
3. Cabling disk shelves to the bridges on page 33
4. Cabling the FC-to-SAS bridges to the controller module in a two-node bridge-attached MetroCluster configuration on page 38

Enabling IP port access on the FibreBridge 7600N bridge if necessary

If you are using an ONTAP version prior to 9.5, or otherwise plan to use out-of-band access to the FibreBridge 7600N bridge using telnet or other IP port protocols and services (FTP, ExpressNAV, ICMP, or QuickNAV), you can enable the access services via the console port.

About this task

Unlike the ATTO FibreBridge 7500N and 6500N bridges, the FibreBridge 7600N bridge is shipped with all IP port protocols and services disabled.

Starting with ONTAP 9.5, *in-band management* of the bridges is supported. This means the bridges can be configured and monitored from the ONTAP CLI via the FC connection to the bridge. Physical access to the bridge via the bridge Ethernet ports is not required and the bridge user interfaces are not required.

This task is required if you have FibreBridge 7600N bridges and you are running ONTAP 9.5 or later and are **not** planning on using in-band management to manage the bridges. Therefore, you need to configure the bridge via the Ethernet management port.
Steps

1. Access the bridge's console interface by connecting a serial cable to the serial port on the FibreBridge 7600N bridge.

2. Using the console, enable the access services, and then save the configuration:
   
   ```
   set closeport none
   saveconfiguration
   ```
   
   The `set closeport none` command enables all access services on the bridge.

3. Disable specific services, if desired, and then save the configuration:
   
   ```
   set closeport service
   saveconfiguration
   ```
   
   `service` can specify one of the following:
   
   - expressnav
   - ftp
   - icmp
   - quicknav
   - snmp
   - telnet
   
   You can check whether a specific protocol is enabled or disabled by using the `get closeport` command.

Configuring the FC-to-SAS bridges

Before cabling your model of the FC-to-SAS bridges, you must configure the settings in the FibreBridge software.

Before you begin

You should decide whether you will be using in-band management of the bridges.

About this task

If you will be using in-band management of the bridge rather than IP management, the steps for configuring the Ethernet port and IP settings can be skipped, as noted in the relevant steps.

Steps

1. If configuring for in-band management, connect a cable from FibreBridge RS-232 serial port to the serial (COM) port on a personal computer.

   The serial connection will be used for initial configuration, and then in-band management via ONTAP and the FC ports can be used to monitor and manage the bridge.

2. If configuring for IP management, connect the Ethernet management 1 port on each bridge to your network by using an Ethernet cable.

   In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than the Ethernet port.

   The Ethernet management 1 port enables you to quickly download the bridge firmware (using ATTO ExpressNA V or FTP management interfaces) and to retrieve core files and extract logs.
3. If configuring for IP management, configure the Ethernet management 1 port for each bridge by following the procedure in section 2.0 of the *ATTO FibreBridge Installation and Operation Manual* for your bridge model.

In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than the Ethernet port.

When running QuickNAV to configure an Ethernet management port, only the Ethernet management port that is connected by the Ethernet cable is configured. For example, if you also wanted to configure the Ethernet management 2 port, you would need to connect the Ethernet cable to port 2 and run QuickNAV.

4. Configure the bridge.

You should make note of the user name and password that you designate.

**Note:** Do not configure time synchronization on ATTO FibreBridge 7600N or 7500N. The time synchronization for ATTO FibreBridge 7600N or 7500N is set to the cluster time after the bridge is discovered by ONTAP. It is also synchronized periodically once a day. The time zone used is GMT and is not changeable.

a. If configuring for IP management, configure the IP settings of the bridge.

In systems running ONTAP 9.5 or later, in-band management can be used to access the bridge via the FC ports rather than via IP access.

To set the IP address without the QuickNAV utility, you need to have a serial connection to the FibreBridge.

**Example**

If using the CLI, you must run the following commands:

```
set ipaddress mp1 ip-address
set ipsubnetmask mp1 subnet-mask
set ipgateway mp1 x.x.x.x
set ipdhcp mp1 disabled
set ethernetspeed mp1 1000
```

b. Configure the bridge name.

The bridges should each have a unique name within the MetroCluster configuration.

Example bridge names for one stack group on each site:

* bridge_A_1a
* bridge_A_1b
* bridge_B_1a
* bridge_B_1b

**Example**

If using the CLI, you must run the following command:

```
set bridgename bridgename
```

c. If running ONTAP 9.4 or earlier, enable SNMP on the bridge:

```
set SNMP enabled
```

If running ONTAP 9.5 or later, ONTAP will use in-band monitoring via the FC connection to the bridge, so you should leave SNMP disabled.
5. Configure the bridge FC ports.
   a. Configure the data rate/speed of the bridge FC ports.
      The supported FC data rate depends on your model bridge.
      - The FibreBridge 7600 bridge supports up to 32, 16, or 8 Gbps.
      - The FibreBridge 7500 bridge supports up to 16, 8, or 4 Gbps.
      - The FibreBridge 6500 bridge supports up to 8, 4, or 2 Gbps.
      **Note:** The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the FC port of the controller module or switch to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

      **Example**
      If using the CLI, you must run the following command:
      ```
      set FCDataRate port-number port-speed
      ```
   b. If you are configuring a FibreBridge 7500N or 6500N bridge, configure the connection mode that the port uses to ptp.
      **Note:** The FCConnMode setting is not required when configuring a FibreBridge 7600N bridge.

      **Example**
      If using the CLI, you must run the following command:
      ```
      set FCConnMode port-number ptp
      ```
   c. If you are configuring a FibreBridge 7600N or 7500N bridge, you must configure or disable the FC2 port.
      - If you are using the second port, you must repeat the previous substeps for the FC2 port.
      - If you are not using the second port, then you must disable the port:
        ```
        FCPortDisable port-number
        ```
      **Example**
      The following example shows the disabling of FC port 2:
      ```
      FCPortDisable 2
      Fibre Channel Port 2 has been disabled.
      ```
   d. If you are configuring a FibreBridge 7600N or 7500N bridge, disable the unused SAS ports:
      ```
      SASPortDisable sas-port
      ```
      **Note:** SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used.

      **Example**
      If only SAS port A is used, then SAS ports B, C, and D must be disabled. The following example shows the disabling of SAS port B. You must similarly disable SAS ports C and D:
6. Save the bridge's configuration and secure access to the bridge.

   a. Save the bridge's configuration.

   **Example**

   You must run the following commands:

   `SaveConfiguration`
   `FirmwareRestart`

   You are prompted to restart the bridge.

   b. If running ONTAP 9.5 or later and configuring for in-band management, secure access to the bridge.

   Starting with ONTAP 9.5, you can secure access to the bridge to allow access only using in-band management through the FC ports.

   **Example**

   You must run the following command:

   `SecureBridge`

7. After completing MetroCluster configuration, use the `flashimages` command to check your version of FibreBridge firmware and, if the bridges are not using the latest supported version, update the firmware on all bridges in the configuration.

   **MetroCluster Service Guide**

   Related concepts

   *In-band management of the FC-to-SAS bridges* on page 27

**Cabling disk shelves to the bridges**

You must use the correct FC-to-SAS bridges for cabling your disk shelves.

**Choices**

- Cabling a FibreBridge 7600N or 7500N bridge with disk shelves using IOM12 modules on page 33
- Cabling a FibreBridge 7600N or 7500N bridge with shelves using IOM6 or IOM3 modules on page 35
- Cabling a FibreBridge 6500N bridge with disk shelves using IOM6 or IOM3 modules on page 37

**Cabling a FibreBridge 7600N or 7500N bridge with disk shelves using IOM12 modules**

After configuring the bridge, you can start cabling your new system.

**About this task**

For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).
Steps

1. Daisy-chain the disk shelves in each stack:
   a. Beginning with the logical first shelf in the stack, connect IOM A port 3 to the next shelf's IOM A port 1 until each IOM A in the stack is connected.
   b. Repeat the previous substep for IOM B.
   c. Repeat the previous substeps for each stack.

   The Installation and Service Guide for your disk shelf model provides detailed information about daisy-chaining disk shelves.

2. Power on the disk shelves, and then set the shelf IDs.
   - You must power-cycle each disk shelf.
   - Shelf IDs must be unique for each SAS disk shelf within the entire MetroCluster configuration (including both sites).

3. Cable disk shelves to the FibreBridge bridges.
   a. For the first stack of disk shelves, cable IOM A of the first shelf to SAS port A on FibreBridge A, and cable IOM B of the last shelf to SAS port A on FibreBridge B.
   b. For additional shelf stacks, repeat the previous step using the next available SAS port on the FibreBridge bridges, using port B for the second stack, port C for the third stack, and port D for the fourth stack.
   c. During cabling, attach the stacks based on IOM12 and IOM3/IOM6 modules to the same bridge as long as they are connected to separate SAS ports.

      Note: Each stack can use different models of IOM, but all disk shelves within a stack must use the same model.

The following illustration shows disk shelves connected to a pair of FibreBridge 7600N or 7500N bridges:
Cabling a FibreBridge 7600N or 7500N bridge with shelves using IOM6 or IOM3 modules

After configuring the bridge, you can start cabling your new system. The FibreBridge 7600N or 7500N bridge uses mini-SAS connectors and supports shelves that use IOM6 or IOM3 modules.

About this task

IOM3 modules are not supported with FibreBridge 7600N bridges.

For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

Steps

1. Daisy-chain the shelves in each stack.
   a. For the first stack of shelves, cable IOM A square port of the first shelf to SAS port A on FibreBridge A.
   b. For the first stack of shelves, cable IOM B circle port of the last shelf to SAS port A on FibreBridge B.

The Installation and Service Guide for your shelf model provides detailed information about daisy-chaining shelves.

SAS Disk Shelves Installation and Service Guide for DS4243, DS2246, DS4486, and DS4246
The following illustration shows a set of bridges cabled to a stack of shelves:

2. For additional shelf stacks, repeat the previous steps using the next available SAS port on the FibreBridge bridges, using port B for a second stack, port C for a third stack, and port D for a fourth stack.

The following illustration shows four stacks connected to a pair of FibreBridge 7600N or 7500N bridges.
Cabling a FibreBridge 6500N bridge with disk shelves using IOM6 or IOM3 modules

After configuring the bridge, you can start cabling your new system. The FibreBridge 6500N bridge uses QSFP connectors.

About this task

Wait at least 10 seconds before connecting the port. The SAS cable connectors are keyed; when oriented correctly into a SAS port, the connector clicks into place and the disk shelf SAS port LNK LED illuminates green. For disk shelves, you insert a SAS cable connector with the pull tab oriented down (on the underside of the connector).

The FibreBridge 6500N bridge does not support disk shelves that use IOM12.

Steps

1. Daisy-chain the disk shelves in each stack.
   For information about daisy-chaining disk shelves, see the Installation and Service Guide for your disk shelf model.

2. For each stack of disk shelves, cable the IOM A square port of the first shelf to the SAS port A on FibreBridge A.

3. For each stack of disk shelves, cable the IOM B circle port of the last shelf to the SAS port A on FibreBridge B.

   Each bridge has one path to its stack of disk shelves: bridge A connects to the A-side of the stack through the first shelf, and bridge B connects to the B-side of the stack through the last shelf.

Example

   Note: The SAS port B bridge is disabled.

The following illustration shows a set of bridges cabled to a stack of four disk shelves:
Cabling the FC-to-SAS bridges to the controller module in a two-node bridge-attached MetroCluster configuration

You must cable the bridges to the controller module in a two-node bridge-attached MetroCluster configuration.

Steps

1. Verify that each bridge can detect all of the disk drives and disk shelves to which the bridge is connected.

<table>
<thead>
<tr>
<th>If you are using the...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTO ExpressNAV GUI</td>
<td>a. In a supported web browser, enter the IP address of a bridge in the browser box. You are brought to the ATTO FibreBridge homepage of the bridge for which you entered the IP address, which has a link.</td>
</tr>
<tr>
<td></td>
<td>b. Click the link, and then enter your user name and the password that you designated when you configured the bridge. The ATTO FibreBridge status page of the bridge appears with a menu to the left.</td>
</tr>
<tr>
<td></td>
<td>c. Click Advanced in the menu.</td>
</tr>
<tr>
<td></td>
<td>d. Run the following command, and then click Submit:</td>
</tr>
<tr>
<td></td>
<td><code>sastargets</code></td>
</tr>
<tr>
<td>Serial port connection</td>
<td>Run the following command:</td>
</tr>
<tr>
<td></td>
<td><code>sastargets</code></td>
</tr>
</tbody>
</table>

   The `sastargets` command output shows the devices (disks and disk shelves) that the bridge is connected to. Output lines are sequentially numbered so that you can quickly count the devices.

   Note: If the text `response truncated` appears at the beginning of the output, you can use Telnet to connect to the bridge and run the same command to view all of the output.

   Example

   The following output shows that 10 disks are connected:

<table>
<thead>
<tr>
<th>Tgt</th>
<th>VendorID</th>
<th>ProductID</th>
<th>Type</th>
<th>SerialNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1CLEE000009940UHJV</td>
</tr>
<tr>
<td>1</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1ELF600009940V1BV</td>
</tr>
<tr>
<td>2</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G3E000009940U2M0</td>
</tr>
<tr>
<td>3</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1EWMP000009940U1X5</td>
</tr>
<tr>
<td>4</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1F2LE000009940G8YU</td>
</tr>
<tr>
<td>5</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FZLF000009940T2K2</td>
</tr>
<tr>
<td>6</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1CEB400009939MGXL</td>
</tr>
<tr>
<td>7</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1G7A900009939FNTT</td>
</tr>
<tr>
<td>8</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FY0700009940GBP</td>
</tr>
<tr>
<td>9</td>
<td>NETAPP</td>
<td>X410_S15K6288A15</td>
<td>DISK</td>
<td>3QP1FXW600009940VERQ</td>
</tr>
</tbody>
</table>

2. Verify that the command output shows that the bridge is connected to all of the disks and disk shelves in the stack that it is supposed to be connected to.

<table>
<thead>
<tr>
<th>If the output is...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct</td>
<td>Repeat Step 1 on page 38 for each remaining bridge.</td>
</tr>
</tbody>
</table>
3. Cable each bridge to the controller modules:

   a. Cable FC port 1 of the bridge to an FC port on the controller module in cluster_A.

   b. Cable FC port 2 of the bridge to an FC port on the controller module in cluster_B.

   If the controller module is configured with a quad-port FC adapter, you should ensure that the storage stacks are connected to two FC ports that are not on the same ASIC. Port a and port b share the same ASIC, and port c and port d share the same ASIC. You should not connect a stack of shelves to port a and port b. Instead, you should use port a and port c, or you should use port b and port d to avoid a single point of failure if an ASIC fails.

   If the controller module is configured with more than one FC adapter, you should not cable both bridge ports to the same adapter. You should distribute FC port 1 to adapter A and FC port 2 to adapter B to avoid a single point of failure.

Example

4. Repeat Step 3 on page 39 on the other bridges until all of the bridges have been cabled.
Configuring the MetroCluster software in ONTAP

You must set up each node in the MetroCluster configuration in ONTAP, including the node-level configurations and the configuration of the nodes into two sites. You must also implement the MetroCluster relationship between the two sites.

Steps
1. Gathering required information on page 41
2. Similarities and differences between standard cluster and MetroCluster configurations on page 44
3. Restoring system defaults and configuring the HBA type on a previously used controller module on page 45
4. Configuring FC-VI ports on a X1132A-R6 quad-port card on FAS8020 systems on page 46
5. Verifying disk assignment in Maintenance mode in a two-node configuration on page 48
6. Verifying the HA state of components on page 49
7. Setting up ONTAP in a two-node MetroCluster configuration on page 50
8. Configuring the clusters into a MetroCluster configuration on page 52
9. Checking for MetroCluster configuration errors with Config Advisor on page 68
10. Verifying switchover, healing, and switchback on page 68
11. Installing the MetroCluster Tiebreaker software on page 68
Gathering required information

You need to gather the required IP addresses for the controller modules before you begin the configuration process.

IP network information worksheet for site A

You must obtain IP addresses and other network information for the first MetroCluster site (site A) from your network administrator before you configure the system.

Site A cluster creation information

When you first create the cluster, you need the following information:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td>Example used in this guide:</td>
</tr>
<tr>
<td></td>
<td>site_A</td>
</tr>
<tr>
<td>DNS domain</td>
<td></td>
</tr>
<tr>
<td>DNS name servers</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Administrator password</td>
<td></td>
</tr>
</tbody>
</table>

Site A node information

For each node in the cluster, you need a management IP address, a network mask, and a default gateway.

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example used in this</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>guide: controller_A_1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not required if using</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>two-node MetroCluster</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(one node at each site)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example used in this</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>guide: controller_A_2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Site A LIFs and ports for cluster peering

For each node in the cluster, you need the IP addresses of two intercluster LIFs, including a network mask and a default gateway. The intercluster LIFs are used to peer the clusters.
### Site A time server information
You must synchronize the time, which requires one or more NTP time servers.

<table>
<thead>
<tr>
<th>Node</th>
<th>Host name</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP server 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Site A AutoSupport information
You must configure AutoSupport on each node, which requires the following information:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>From email address</td>
<td>IP addresses or names</td>
</tr>
<tr>
<td>Mail hosts</td>
<td>HTTP, HTTPS, or SMTP</td>
</tr>
<tr>
<td>Transport protocol</td>
<td>Proxy server</td>
</tr>
<tr>
<td>Recipient email addresses or distribution lists</td>
<td>Full-length messages</td>
</tr>
<tr>
<td></td>
<td>Concise messages</td>
</tr>
<tr>
<td></td>
<td>Partners</td>
</tr>
</tbody>
</table>

### Site A SP information
You must enable access to the Service Processor (SP) of each node for troubleshooting and maintenance, which requires the following network information for each node:

<table>
<thead>
<tr>
<th>Node</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### IP network information worksheet for site B
You must obtain IP addresses and other network information for the second MetroCluster site (site B) from your network administrator before you configure the system.

### Site B cluster creation information
When you first create the cluster, you need the following information:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td></td>
</tr>
<tr>
<td>Example used in this guide: site_B</td>
<td></td>
</tr>
<tr>
<td>DNS domain</td>
<td></td>
</tr>
<tr>
<td>Type of information</td>
<td>Your values</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>DNS name servers</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Administrator password</td>
<td></td>
</tr>
</tbody>
</table>

**Site B node information**

For each node in the cluster, you need a management IP address, a network mask, and a default gateway.

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1</td>
<td></td>
<td>controller_B_1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 2</td>
<td></td>
<td>controller_B_2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Site B LIFs and ports for cluster peering**

For each node in the cluster, you need the IP addresses of two intercluster LIFs, including a network mask and a default gateway. The intercluster LIFs are used to peer the clusters.

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IP address of intercluster LIF</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 IC LIF 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Node 1 IC LIF 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Site B time server information**

You must synchronize the time, which requires one or more NTP time servers.

<table>
<thead>
<tr>
<th>Node</th>
<th>Host name</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP server 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP server 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Site B AutoSupport information**

You must configure AutoSupport on each node, which requires the following information:

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Your values</th>
</tr>
</thead>
<tbody>
<tr>
<td>From email address</td>
<td></td>
</tr>
</tbody>
</table>
### Site B SP information

You must enable access to the Service Processor (SP) of each node for troubleshooting and maintenance, which requires the following network information for each node:

<table>
<thead>
<tr>
<th>Node</th>
<th>IP address</th>
<th>Network mask</th>
<th>Default gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 (controller_B_1)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Similarities and differences between standard cluster and MetroCluster configurations

The configuration of the nodes in each cluster in a MetroCluster configuration is similar to that of nodes in a standard cluster.

The MetroCluster configuration is built on two standard clusters. Physically, the configuration must be symmetrical, with each node having the same hardware configuration, and all of the MetroCluster components must be cabled and configured. However, the basic software configuration for nodes in a MetroCluster configuration is the same as that for nodes in a standard cluster.

<table>
<thead>
<tr>
<th>Configuration step</th>
<th>Standard cluster configuration</th>
<th>MetroCluster configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure management, cluster, and data LIFs on each node.</td>
<td>Same in both types of clusters</td>
<td>Same in both types of clusters</td>
</tr>
<tr>
<td>Configure the root aggregate.</td>
<td>Same in both types of clusters</td>
<td>Same in both types of clusters</td>
</tr>
<tr>
<td>Set up the cluster on one node in the cluster.</td>
<td>Same in both types of clusters</td>
<td>Same in both types of clusters</td>
</tr>
<tr>
<td>Join the other node to the cluster.</td>
<td>Same in both types of clusters</td>
<td>Same in both types of clusters</td>
</tr>
<tr>
<td>Create a mirrored root aggregate.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Peer the clusters.</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Enable the MetroCluster configuration.</td>
<td>Does not apply</td>
<td>Required</td>
</tr>
</tbody>
</table>
Restoring system defaults and configuring the HBA type on a previously used controller module

If your controller modules have been used previously, you must reset them for a successful MetroCluster configuration. This task is only required for stretch configurations using FC-to-SAS bridges.

About this task

Important: This task is required only on controller modules that have been previously configured. You do not need to perform this task if you received the controller modules from the factory.

Steps

1. At the LOADER prompt, return the environmental variables to their default setting:
   
   ```
   set-defaults
   ```

2. Boot the node into Maintenance mode, and then configure the settings for any HBAs in the system:

<table>
<thead>
<tr>
<th>If you have this type of HBA and desired mode...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNA FC</td>
<td>ucadmin modify -m fc -t initiator adapter_name</td>
</tr>
<tr>
<td>CNA Ethernet</td>
<td>ucadmin modify -mode cna adapter_name</td>
</tr>
<tr>
<td>FC target</td>
<td>fcadmin config -t target adapter_name</td>
</tr>
<tr>
<td>FC initiator</td>
<td>fcadmin config -t initiator adapter_name</td>
</tr>
</tbody>
</table>

3. Exit Maintenance mode:
   
   ```
   halt
   ```

   After you run the command, wait until the node stops at the LOADER prompt.

4. Boot the node back into Maintenance mode to enable the configuration changes to take effect.

5. Verify the changes you made:

<table>
<thead>
<tr>
<th>If you have this type of HBA...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNA</td>
<td>ucadmin show</td>
</tr>
<tr>
<td>FC</td>
<td>fcadmin show</td>
</tr>
</tbody>
</table>

6. Exit Maintenance mode:

   ```
   halt
   ```

   After you run the command, wait until the node stops at the LOADER prompt.

7. Boot the node to the boot menu:

   ```
   boot_ontap menu
   ```

   After you run the command, wait until the boot menu is shown.

8. Clear the node configuration by typing `wipeconfig` at the boot menu prompt, and then press Enter.
The following screen shows the boot menu prompt:

```
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
Selection (1-9)? wipeconfig
This option deletes critical system configuration, including cluster membership.
Warning: do not run this option on a HA node that has been taken over.
Are you sure you want to continue?: yes
Rebooting to finish wipeconfig request.
```

### Configuring FC-VI ports on a X1132A-R6 quad-port card on FAS8020 systems

If you are using the X1132A-R6 quad-port card on a FAS8020 system, you can enter Maintenance mode to configure the 1a and 1b ports for FC-VI and initiator usage. This is not required on MetroCluster systems received from the factory, in which the ports are set appropriately for your configuration.

**About this task**

This task must be performed in Maintenance mode.

**Steps**

1. Disable the ports:
   ```
   storage disable adapter 1a
   storage disable adapter 1b
   ```

   **Example**

   ```
   *> storage disable adapter 1a
   Jun 03 02:17:57 [controller_B_1:fci.adapter.offlining:info]:
   Offlining Fibre Channel adapter 1a.
   Host adapter 1a disable succeeded
   Jun 03 02:17:57 [controller_B_1:fci.adapter.offline:info]: Fibre Channel adapter 1a is now offline.
   *> storage disable adapter 1b
   Jun 03 02:18:43 [controller_B_1:fci.adapter.offlining:info]:
   Offlining Fibre Channel adapter 1b.
   Host adapter 1b disable succeeded
   Jun 03 02:18:43 [controller_B_1:fci.adapter.offline:info]: Fibre Channel adapter 1b is now offline.
   *> 
   ```

2. Verify that the ports are disabled:
   ```
   ucadmin show
   ```
3. Set the a and b ports to FC-VI mode:

```
ucadmin modify -adapter 1a -type fcvi
```

The command sets the mode on both ports in the port pair, 1a and 1b (even though only 1a is specified in the command).

Example

```
*> ucadmin modify -t fcvi 1a
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has changed to fcvi on adapter 1a. Reboot the controller for the changes to take effect.
Jun 03 02:19:13 [controller_B_1:ucm.type.changed:info]: FC-4 type has changed to fcvi on adapter 1b. Reboot the controller for the changes to take effect.
```

4. Confirm that the change is pending:

```
ucadmin show
```

Example

```
*> ucadmin show
```

<table>
<thead>
<tr>
<th>Adapter</th>
<th>Mode</th>
<th>Type</th>
<th>Current Mode</th>
<th>Current Type</th>
<th>Pending Mode</th>
<th>Pending Type</th>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>fcvi</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>1b</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>fcvi</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>1c</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>online</td>
<td></td>
</tr>
<tr>
<td>1d</td>
<td>fc</td>
<td>initiator</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>online</td>
<td></td>
</tr>
</tbody>
</table>

5. Shut down the controller, and then reboot into Maintenance mode.

6. Confirm the configuration change:

```
ucadmin show local
```

Example

```
*> ucadmin show local
```

<table>
<thead>
<tr>
<th>Node</th>
<th>Adapter</th>
<th>Mode</th>
<th>Type</th>
<th>Mode</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>controller_B_1</td>
<td>la</td>
<td>fc</td>
<td>fcvi</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
<tr>
<td>controller_B_1</td>
<td>lb</td>
<td>fc</td>
<td>fcvi</td>
<td>-</td>
<td>-</td>
<td>online</td>
</tr>
</tbody>
</table>
Verifying disk assignment in Maintenance mode in a two-node configuration

Before fully booting the system to ONTAP, you can optionally boot the system to Maintenance mode and verify the disk assignment on the nodes. The disks should be assigned to create a fully symmetric configuration with both sites owning their own disk shelves and serving data, where each node and each pool have an equal number of mirrored disks assigned to them.

Before you begin
The system must be in Maintenance mode.

About this task
New MetroCluster systems have disk assignment completed prior to shipment.

The following table shows example pool assignments for a MetroCluster configuration. Disks are assigned to pools on a per-shelf basis.

<table>
<thead>
<tr>
<th>Disk shelf (example name)...</th>
<th>At site...</th>
<th>Belongs to...</th>
<th>And is assigned to that node's...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk shelf 1 (shelf_A_1_1)</td>
<td>Site A</td>
<td>Node A 1</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 2 (shelf_A_1_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 3 (shelf_B_1_1)</td>
<td></td>
<td>Node B 1</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 4 (shelf_B_1_3)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 9 (shelf_B_1_2)</td>
<td>Site B</td>
<td>Node B 1</td>
<td>Pool 0</td>
</tr>
<tr>
<td>Disk shelf 10 (shelf_B_1_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk shelf 11 (shelf_A_1_2)</td>
<td></td>
<td>Node A 1</td>
<td>Pool 1</td>
</tr>
<tr>
<td>Disk shelf 12 (shelf_A_1_4)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If your configuration includes DS460C disk shelves, you should manually assign the disks using the following guidelines for each 12-disk drawer:

<table>
<thead>
<tr>
<th>Assign these disks in the drawer...</th>
<th>To this node and pool...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 6</td>
<td>Local node's pool 0</td>
</tr>
<tr>
<td>7 - 12</td>
<td>DR partner's pool 1</td>
</tr>
</tbody>
</table>

This disk assignment pattern minimizes the effect on an aggregate if a drawer goes offline.
Steps

1. If your system was received from the factory, confirm the shelf assignments:
   
   ```bash
disk show -v
   ```

2. If necessary, you can explicitly assign disks on the attached disk shelves to the appropriate pool
   by using the `disk assign` command.

   Disk shelves at the same site as the node are assigned to pool 0 and disk shelves located at the
   partner site are assigned to pool 1. You should assign an equal number of shelves to each pool.

   a. If you have not done so, boot each system into Maintenance mode.

   b. On the node on site A, systematically assign the local disk shelves to pool 0 and the remote
disk shelves to pool 1:

   ```bash
disk assign -shelf disk_shelf_name -p pool
   ```

   Example

   If storage controller node_A_1 has four shelves, you issue the following commands:

   ```bash
*> disk assign -shelf shelf_A_1_1 -p 0
*> disk assign -shelf shelf_A_1_3 -p 0
*> disk assign -shelf shelf_A_1_2 -p 1
*> disk assign -shelf shelf_A_1_4 -p 1
   ```

c. On the node at the remote site (site B), systematically assign its local disk shelves to pool 0
   and its remote disk shelves to pool 1:

   ```bash
disk assign -shelf disk_shelf_name -p pool
   ```

   Example

   If storage controller node_B_1 has four shelves, you issue the following commands:

   ```bash
*> disk assign -shelf shelf_B_1_2 -p 0
*> disk assign -shelf shelf_B_1_4 -p 0
*> disk assign -shelf shelf_B_1_1 -p 1
*> disk assign -shelf shelf_B_1_3 -p 1
   ```

d. Show the disk shelf IDs and bays for each disk:

   ```bash
disk show -v
   ```

Verifying the HA state of components

In a stretch MetroCluster configuration that is not preconfigured at the factory, you must verify that
the HA state of the controller and chassis component is set to `mcc-2n` so that they boot up properly.
For systems received from the factory, this value is preconfigured and you do not need to verify it.

Before you begin

The system must be in Maintenance mode.
Steps

1. In Maintenance mode, view the HA state of the controller module and chassis:
   
   `ha-config show`
   
   The controller module and chassis should show the value `mcc-2n`.

2. If the displayed system state of the controller is not `mcc-2n`, set the HA state for the controller:
   
   `ha-config modify controller mcc-2n`

3. If the displayed system state of the chassis is not `mcc-2n`, set the HA state for the chassis:
   
   `ha-config modify chassis mcc-2n`
   
   a. Halt the node.
   
   b. Wait until the node is back at the LOADER prompt.

4. Repeat these steps on each node in the MetroCluster configuration.

Setting up ONTAP in a two-node MetroCluster configuration

In a two-node MetroCluster configuration, on each cluster you must boot up the node, exit the Node Setup wizard, and use the Cluster Setup wizard to configure the node into a single-node cluster.

Before you begin

You must not have configured the Service Processor.

About this task

This task is for two-node MetroCluster configurations using native NetApp storage.

New MetroCluster systems are preconfigured; you do not need to perform these steps. However, you should configure AutoSupport.

This task must be performed on both clusters in the MetroCluster configuration.

For more general information about setting up ONTAP, see the *Software Setup Guide.*

Steps

1. Power on the first node.

   The node boots, and then the Node Setup wizard starts on the console, informing you that AutoSupport will be enabled automatically.

   Welcome to node setup.
   
   You can enter the following commands at any time:
   
   "help" or "?" - if you want to have a question clarified,
   "back" - if you want to change previously answered questions, and
   "exit" or "quit" - if you want to quit the setup wizard.
   
   Any changes you made before quitting will be saved.
   
   To accept a default or omit a question, do not enter a value.

   This system will send event messages and weekly reports to NetApp Technical Support. To disable this feature, enter "autosupport modify -support disable" within 24 hours. Enabling AutoSupport can significantly speed problem...
determination and resolution should a problem occur on your system. For further information on AutoSupport, see: http://support.netapp.com/autosupport/

Type yes to confirm and continue {yes}:

2. Because you are using the CLI to set up the cluster, exit the Node Setup wizard:
   ```
   exit
   ```
   The Node Setup might be used to configure the node's node management interface for use with the Cluster Setup wizard.

   The Node Setup wizard exits, and a login prompt appears, warning that you have not completed the setup tasks.

   Exiting the node setup wizard. Any changes you made have been saved.

   Warning: You have exited the node setup wizard before completing all of the tasks. The node is not configured. You can complete node setup by typing "node setup" in the command line interface.

   login:

3. Log in to the admin account by using the admin user name.

4. Start the Cluster Setup wizard:
   ```
   cluster setup
   ```
   ::> cluster setup

   Welcome to the cluster setup wizard.

   You can enter the following commands at any time:
   "help" or "?" - if you want to have a question clarified,
   "back" - if you want to change previously answered questions, and
   "exit" or "quit" - if you want to quit the cluster setup wizard.
   Any changes you made before quitting will be saved.

   You can return to cluster setup at any time by typing "cluster setup".
   To accept a default or omit a question, do not enter a value.

   Do you want to create a new cluster or join an existing cluster? {create, join}:

5. Create a new cluster:
   ```
   create
   ```

6. Accept the system defaults by pressing Enter, or enter your own values by typing no, and then pressing Enter.

7. Follow the prompts to complete the Cluster Setup wizard, pressing Enter to accept the default values or typing your own values and then pressing Enter.

   The default values are determined automatically based on your platform and network configuration.

8. After you complete the Cluster Setup wizard and it exits, verify that the cluster is active and the first node is healthy:
   ```
   cluster show
   ```
Example

The following example shows a cluster in which the first node (cluster1-01) is healthy and eligible to participate:

```bash
cluster1::> cluster show
  Node               Health  Eligibility
                   ------------   -----------
cluster1-01       true      true
```

If it becomes necessary to change any of the settings you entered for the admin SVM or node SVM, you can access the Cluster Setup wizard by using the `cluster setup` command.

Related information

*Software setup*

Configuring the clusters into a MetroCluster configuration

You must peer the clusters, mirror the root aggregates, create a mirrored data aggregate, and then issue the command to implement the MetroCluster operations.

Peering the clusters

The clusters in the MetroCluster configuration must be in a peer relationship so that they can communicate with each other and perform the data mirroring essential to MetroCluster disaster recovery.

Steps

1. Configuring intercluster LIFs on page 52
2. Creating a cluster peer relationship on page 56

Related concepts

* Considerations when using dedicated ports on page 9
* Considerations when sharing data ports on page 9

Related information

* Cluster and SVM peering express configuration

Configuring intercluster LIFs

You must create intercluster LIFs on ports used for communication between the MetroCluster partner clusters. You can use dedicated ports or ports that also have data traffic.

Choices

* Configuring intercluster LIFs on dedicated ports on page 53
* Configuring intercluster LIFs on shared data ports on page 55
Configuring intercluster LIFs on dedicated ports

You can configure intercluster LIFs on dedicated ports. Doing so typically increases the available bandwidth for replication traffic.

Steps

1. List the ports in the cluster:

   `network port show`

   For complete command syntax, see the man page.

   **Example**

   The following example shows the network ports in `cluster01`:

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast</th>
<th>Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster01-01</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td>cluster01-02</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td></td>
</tr>
</tbody>
</table>

2. Determine which ports are available to dedicate to intercluster communication:

   `network interface show -fields home-port,curr-port`

   For complete command syntax, see the man page.

   **Example**

   The following example shows that ports `e0e` and `e0f` have not been assigned LIFs:

<table>
<thead>
<tr>
<th>vserver lif</th>
<th>home-port</th>
<th>curr-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster cluster01-01_clus1</td>
<td>e0a</td>
<td>e0a</td>
</tr>
<tr>
<td>Cluster cluster01-01_clus2</td>
<td>e0b</td>
<td>e0b</td>
</tr>
<tr>
<td>Cluster cluster01-02_clus1</td>
<td>e0a</td>
<td>e0a</td>
</tr>
<tr>
<td>Cluster cluster01-02_clus2</td>
<td>e0b</td>
<td>e0b</td>
</tr>
<tr>
<td>cluster01</td>
<td>cluster_mgmt</td>
<td>e0c</td>
</tr>
<tr>
<td>cluster01</td>
<td>cluster01-01_mgmt1</td>
<td>e0c</td>
</tr>
<tr>
<td>cluster01</td>
<td>cluster01-02_mgmt1</td>
<td>e0c</td>
</tr>
</tbody>
</table>

3. Create a failover group for the dedicated ports:

   `network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical_or_logical_ports`

   **Example**

   The following example assigns ports `e0e` and `e0f` to the failover group `intercluster01` on the system SVM `cluster01`:
4. Verify that the failover group was created:

```bash
network interface failover-groups show
```

For complete command syntax, see the man page.

**Example**

```bash
cluster01::> network interface failover-groups show
```

<table>
<thead>
<tr>
<th>Failover</th>
<th>Vserver</th>
<th>Group</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster</td>
<td>cluster01</td>
<td>Cluster</td>
<td>cluster01-01:e0a, cluster01-01:e0b, cluster01-02:e0a, cluster01-02:e0b</td>
</tr>
<tr>
<td></td>
<td>cluster01</td>
<td>Default</td>
<td>cluster01-01:e0a, cluster01-01:e0d, cluster01-02:e0a, cluster01-02:e0d</td>
</tr>
<tr>
<td></td>
<td>intercluster01</td>
<td>cluster01</td>
<td>cluster01-01:e0e, cluster01-01:e0f, cluster01-02:e0e, cluster01-02:e0f</td>
</tr>
<tr>
<td></td>
<td>intercluster01</td>
<td>intercluster01</td>
<td>cluster01-01:e0e, cluster01-01:e0f, cluster01-02:e0e, cluster01-02:e0f</td>
</tr>
</tbody>
</table>

5. Create intercluster LIFs on the system SVM and assign them to the failover group:

```bash
network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group
```

For complete command syntax, see the man page.

**Example**

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02` in the failover group `intercluster01`:

```bash
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl01 -role intercluster -home-node cluster01-01 -home-port e0e -address 192.168.1.201 -netmask 255.255.255.0 -failover-group intercluster01
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl02 -role intercluster -home-node cluster01-02 -home-port e0f -address 192.168.1.202 -netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

```bash
network interface show --role intercluster
```

For complete command syntax, see the man page.

**Example**

```bash
cluster01::> network interface show --role intercluster
```

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Current Is Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster01_icl01</td>
<td>up/up</td>
<td>192.168.1.201/24</td>
<td>cluster01-01 e0e</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster01_icl02</td>
<td>up/up</td>
<td>192.168.1.202/24</td>
<td>cluster01-02 e0f</td>
<td>true</td>
<td></td>
</tr>
</tbody>
</table>

7. Verify that the intercluster LIFs are redundant:

```bash
network interface show --role intercluster --failover
```

For complete command syntax, see the man page.

**Example**

```bash
cluster01::> network interface show --role intercluster --failover
```

<table>
<thead>
<tr>
<th>Logical Interface</th>
<th>Status</th>
<th>Network Address/Mask</th>
<th>Current Node</th>
<th>Current Port</th>
<th>Current Is Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster01_icl01</td>
<td>up/up</td>
<td>192.168.1.201/24</td>
<td>cluster01-01 e0e</td>
<td>true</td>
<td></td>
</tr>
<tr>
<td>cluster01_icl02</td>
<td>up/up</td>
<td>192.168.1.202/24</td>
<td>cluster01-02 e0f</td>
<td>true</td>
<td></td>
</tr>
</tbody>
</table>
Example

The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the SVM `e0e` port will fail over to the `e0f` port.

```
cluster01::> network interface show -role intercluster -failover
Vserver Interface Home:Port Failover Policy Failover Group
-------- --------------- --------------------- --------------- --------
cluster01-01 cluster01-01_icl01 cluster01-01:e0e local-only intercluster01
Failover Targets: cluster01-01:e0e, cluster01-01:e0f
cluster01-01 cluster01-01_icl02 cluster01-01-02:e0e local-only intercluster01
Failover Targets: cluster01-02:e0e, cluster01-02:e0f
```

Related concepts

*Considerations when using dedicated ports* on page 9

Configuring intercluster LIFs on shared data ports

You can configure intercluster LIFs on ports shared with the data network. Doing so reduces the number of ports you need for intercluster networking.

Steps

1. List the ports in the cluster:

   `network port show`

   For complete command syntax, see the man page.

Example

The following example shows the network ports in `cluster01`:

```
cluster01::> network port show
Node Port IPspace Broadcast Domain Link MTU Admin/Oper
------ --------- -------------- ----------- ----- ------------
cluster01-01
  e0a Cluster Cluster up 1500 auto/1000
  e0b Cluster Cluster up 1500 auto/1000
  e0c Default Default up 1500 auto/1000
  e0d Default Default up 1500 auto/1000
cluster01-02
  e0a Cluster Cluster up 1500 auto/1000
  e0b Cluster Cluster up 1500 auto/1000
  e0c Default Default up 1500 auto/1000
  e0d Default Default up 1500 auto/1000
```

2. Create intercluster LIFs on the system SVM:

   `network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home-port port -address port_IP -netmask netmask`

   For complete command syntax, see the man page.

Example

The following example creates intercluster LIFs `cluster01_icl01` and `cluster01_icl02`:

```
cluster01::> network interface create -vserver cluster01 -lif cluster01_icl01 -role intercluster -home-node cluster01-01 -home-port e0c -address 192.168.1.201 -netmask 255.255.255.0
```

Configuring the MetroCluster software in ONTAP | 55
3. Verify that the intercluster LIFs were created:

   **network interface show -role intercluster**

   For complete command syntax, see the man page.

   **Example**

   ```bash
   cluster01::> network interface show -role intercluster
   Logical    Status     Network            Current       Current Is
   Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
   ----------- ---------- ---------- ------------------ ------------- ------- ----
   cluster01
   cluster01_icl01 up/up      192.168.1.201/24   cluster01-01  e0c     true
   cluster01_icl02 up/up      192.168.1.202/24   cluster01-02  e0c     true
   ```

4. Verify that the intercluster LIFs are redundant:

   **network interface show -role intercluster -failover**

   For complete command syntax, see the man page.

   **Example**

   The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the `e0c` port will fail over to the `e0d` port.

   ```bash
   cluster01::> network interface show -role intercluster -failover
   Logical         Home                  Failover        Failover
   Vserver  Interface       Node:Port             Policy          Group
   -------- --------------- --------------------- --------------- --------
   cluster01
   cluster01_icl01 cluster01-01:e0c   local-only      192.168.1.201/24
   Failover Targets: cluster01-01:e0c,
   cluster01-01:e0d
   cluster01_icl02 cluster01-02:e0c   local-only      192.168.1.201/24
   Failover Targets: cluster01-02:e0c,
   cluster01-02:e0d
   ```

**Related concepts**

*Considerations when sharing data ports* on page 9

**Creating a cluster peer relationship**

You must create the cluster peer relationship between the MetroCluster clusters.

**Creating a cluster peer relationship**

You can use the `cluster peer create` command to create a peer relationship between a local and remote cluster. After the peer relationship has been created, you can run `cluster peer create` on the remote cluster to authenticate it to the local cluster.

**Before you begin**

- You must have created intercluster LIFs on every node in the clusters that are being peered.
- The clusters must be running ONTAP 9.3 or later.

**About this task**
Steps

1. On the destination cluster, create a peer relationship with the source cluster:

   `cluster peer create -generate-passphrase -offer-expiration MM/DD/YYYY
   HH:MM:SS|1...7days|1...168hours -peer-addrs peer_LIF_IPs -ipspace ipspace`

   If you specify both `-generate-passphrase` and `-peer-addrs`, only the cluster whose
   intercluster LIFs are specified in `-peer-addrs` can use the generated password.

   You can ignore the `-ipspace` option if you are not using a custom IPspace. For complete
   command syntax, see the man page.

   **Example**

   The following example creates a cluster peer relationship on an unspecified remote cluster:

   ```bash
   cluster02::> cluster peer create -generate-passphrase -offer-expiration 2days
   
   Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
   Expiration Time: 6/7/2017 08:16:10 EST
   Initial Allowed Vserver Peers: -
   Intercluster LIF IP: 192.140.112.101
   Peer Cluster Name: Clus_7ShR (temporary generated)
   
   Warning: make a note of the passphrase - it cannot be displayed again.
   ```

2. On source cluster, authenticate the source cluster to the destination cluster:

   `cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace`

   For complete command syntax, see the man page.

   **Example**

   The following example authenticates the local cluster to the remote cluster at intercluster LIF IP
   addresses 192.140.112.101 and 192.140.112.102:

   ```bash
   cluster01::> cluster peer create -peer-addrs 192.140.112.101,192.140.112.102
   
   Notice: Use a generated passphrase or choose a passphrase of 8 or
   more characters.
   To ensure the authenticity of the peering relationship, use a
   phrase or sequence of characters that would be hard to guess.
   
   Enter the passphrase:
   Confirm the passphrase:
   
   Clusters cluster02 and cluster01 are peered.
   ```

   Enter the passphrase for the peer relationship when prompted.

3. Verify that the cluster peer relationship was created:

   `cluster peer show -instance`

   **Example**

   ```bash
   cluster01::> cluster peer show -instance
   
   Peer Cluster Name: cluster02
   Remote Intercluster Addresses: 192.140.112.101,
   192.140.112.102
   ```
Availability of the Remote Cluster: Available
Remote Cluster Name: cluster2
Active IP Addresses: 192.140.112.101, 192.140.112.102
Cluster Serial Number: 1-80-123456
Address Family of Relationship: ipv4
Authentication Status Administrative: no-authentication
Authentication Status Operational: absent
Last Update Time: 02/05 21:05:41
IPspace for the Relationship: Default

4. Check the connectivity and status of the nodes in the peer relationship:

   cluster peer health show

**Example**

```
cluster01:=> cluster peer health show
Node       cluster-Name                Node-Name
Ping-Status               RDB-Health Cluster-Health
Avail...
-------- --------------------------- ---------  ---------------
--------
cluster01-01  cluster02                   cluster02-01
Data: interface_reachable ICMP: interface_reachable true   true    true
cluster01-02  cluster02                   cluster02-01
Data: interface_reachable ICMP: interface_reachable true   true    true
```

Creating a cluster peer relationship (ONTAP 9.2 and earlier)

You can use the `cluster peer create` command to initiate a request for a peering relationship between a local and remote cluster. After the peer relationship has been requested by the local cluster, you can run `cluster peer create` on the remote cluster to accept the relationship.

**Before you begin**

- You must have created intercluster LIFs on every node in the clusters being peered.
- The cluster administrators must have agreed on the passphrase each cluster will use to authenticate itself to the other.

**Steps**

1. On the data protection destination cluster, create a peer relationship with the data protection source cluster:

   `cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace`

   You can ignore the `-ipspace` option if you are not using a custom IPSpace. For complete command syntax, see the man page.

**Example**

The following example creates a cluster peer relationship with the remote cluster at intercluster LIF IP addresses 192.168.2.201 and 192.168.2.202:
Enter the passphrase for the peer relationship when prompted.

2. On the data protection source cluster, authenticate the source cluster to the destination cluster:

```
cluster peer create -peer-addrs peer_LIF_IPs -ipspace ipspace
```

For complete command syntax, see the man page.

**Example**

The following example authenticates the local cluster to the remote cluster at intercluster LIF IP addresses 192.140.112.203 and 192.140.112.204:

```
cluster01::> cluster peer create -peer-addrs 192.168.2.203,192.168.2.204
```

Enter the passphrase for the peer relationship when prompted.

3. Verify that the cluster peer relationship was created:

```
cluster peer show -instance
```

For complete command syntax, see the man page.

**Example**

```
cluster01::> cluster peer show -instance
Peer Cluster Name: cluster01
Remote Intercluster Addresses: 192.168.2.201,192.168.2.202
Availability: Available
Remote Cluster Name: cluster02
Active IP Addresses: 192.168.2.201,192.168.2.202
Cluster Serial Number: 1-80-000013
```

4. Check the connectivity and status of the nodes in the peer relationship:

```
cluster peer health show
```

For complete command syntax, see the man page.

**Example**

```
cluster01::> cluster peer health show
Node  cluster-Name                  Node-Name          Ping-Status     RDB-Health  Cluster-Health  Avail-
---------- --------------------------- ---------  --------------- --------
cluster01-01  cluster02                   cluster02-01  Data: interface_reachable true     true     true
                       ICMP: interface_reachable true     true     true
cluster01-02  cluster02                   cluster02-01  Data: interface_reachable true     true     true
                       ICMP: interface_reachable true     true     true
cluster02-02  cluster02                   cluster02-01  Data: interface_reachable true     true     true
                       ICMP: interface_reachable true     true     true
```
Mirroring the root aggregates

You must mirror the root aggregates to provide data protection.

About this task

By default, the root aggregate is created as RAID-DP type aggregate. You can change the root aggregate from RAID-DP to RAID4 type aggregate. The following command modifies the root aggregate for RAID4 type aggregate:

```
storage aggregate modify -aggregate aggr_name -raidtype raid4
```

**Note:** On non-ADP systems, the RAID type of the aggregate can be modified from the default RAID-DP to RAID4 before or after the aggregate is mirrored.

Steps

1. Mirror the root aggregate:
   ```
   storage aggregate mirror aggr_name
   ```

   **Example**
   The following command mirrors the root aggregate for controller_A_1:
   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```
   This mirrors the aggregate, so it consists of a local plex and a remote plex located at the remote MetroCluster site.

2. Repeat the previous step for each node in the MetroCluster configuration.

Related information

- Logical storage management
- ONTAP concepts

Creating a mirrored data aggregate on each node

You must create a mirrored data aggregate on each node in the DR group.

Before you begin

- You should know what drives or array LUNs will be used in the new aggregate.
- If you have multiple drive types in your system (heterogeneous storage), you should understand how you can ensure that the correct drive type is selected.

About this task

- Drives and array LUNs are owned by a specific node; when you create an aggregate, all drives in that aggregate must be owned by the same node, which becomes the home node for that aggregate.
- Aggregate names should conform to the naming scheme you determined when you planned your MetroCluster configuration.

Disk and aggregate management
Steps

1. Display a list of available spares:

   `storage disk show -spare -owner node_name`

2. Create the aggregate by using the `storage aggregate create -mirror true` command.

   If you are logged in to the cluster on the cluster management interface, you can create an aggregate on any node in the cluster. To ensure that the aggregate is created on a specific node, use the `-node` parameter or specify drives that are owned by that node.

   You can specify the following options:

   • Aggregate's home node (that is, the node that owns the aggregate in normal operation)
   • List of specific drives or array LUNs that are to be added to the aggregate
   • Number of drives to include
     
     Note: In the minimum supported configuration, in which a limited number of drives are available, you must use the force-small-aggregate option to allow the creation of a three disk RAID-DP aggregate.
     
   • Checksum style to use for the aggregate
   • Type of drives to use
   • Size of drives to use
   • Drive speed to use
   • RAID type for RAID groups on the aggregate
   • Maximum number of drives or array LUNs that can be included in a RAID group
   • Whether drives with different RPM are allowed

   For more information about these options, see the `storage aggregate create` man page.

Example

The following command creates a mirrored aggregate with 10 disks:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Verify the RAID group and drives of your new aggregate:

   `storage aggregate show-status -aggregate aggregate-name`

Creating unmirrored data aggregates

You can optionally create unmirrored data aggregates for data that does not require the redundant mirroring provided by MetroCluster configurations.

Before you begin

• You should know what drives or array LUNs will be used in the new aggregate.
• If you have multiple drive types in your system (heterogeneous storage), you should understand how you can verify that the correct drive type is selected.
About this task

Attention:

In MetroCluster FC configurations, the unmirrored aggregates will only be online after a switchover if the remote disks in the aggregate are accessible. If the ISLs fail, the local node may be unable to access the data in the unmirrored remote disks. The failure of an aggregate can lead to a reboot of the local node.

Note: The unmirrored aggregates must be local to the node owning them.

- Drives and array LUNs are owned by a specific node; when you create an aggregate, all drives in that aggregate must be owned by the same node, which becomes the home node for that aggregate.
- Aggregate names should conform to the naming scheme you determined when you planned your MetroCluster configuration.
- The Disks and Aggregates Power Guide contains more information about mirroring aggregates.

Steps

1. Display a list of available spares:
   
   ```bash
   storage disk show --spare --owner node_name
   ```

2. Create the aggregate:

   ```bash
   storage aggregate create
   ```

   If you are logged in to the cluster on the cluster management interface, you can create an aggregate on any node in the cluster. To verify that the aggregate is created on a specific node, you should use the `-node` parameter or specify drives that are owned by that node.

   You can specify the following options:
   - Aggregate's home node (that is, the node that owns the aggregate in normal operation)
   - List of specific drives or array LUNs that are to be added to the aggregate
   - Number of drives to include
   - Checksum style to use for the aggregate
   - Type of drives to use
   - Size of drives to use
   - Drive speed to use
   - RAID type for RAID groups on the aggregate
   - Maximum number of drives or array LUNs that can be included in a RAID group
   - Whether drives with different RPM are allowed

   For more information about these options, see the `storage aggregate create` man page.

Example

The following command creates a unmirrored aggregate with 10 disks:
3. Verify the RAID group and drives of your new aggregate:

```
storage aggregate show-status -aggregate aggregate-name
```

Related information

**Disk and aggregate management**

**Implementing the MetroCluster configuration**

You must run the `metrocluster configure` command to start data protection in a MetroCluster configuration.

**Before you begin**

- There should be at least two non-root mirrored data aggregates on each cluster. Additional data aggregates can be either mirrored or unmirrored. You can verify this with the `storage aggregate show` command.
  
  **Note:** If you want to use a single mirrored data aggregate, then see step 1 on page 63 for instructions.

- The ha-config state of the controllers and chassis must be `mcc-2n`.

**About this task**

You issue the `metrocluster configure` command once, on any of the nodes, to enable the MetroCluster configuration. You do not need to issue the command on each of the sites or nodes, and it does not matter which node or site you choose to issue the command on.

**Steps**

1. Configure the MetroCluster in the following format:

<table>
<thead>
<tr>
<th>If your MetroCluster configuration has...</th>
<th>Then do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple data aggregates</td>
<td>From any node's prompt, configure MetroCluster: <code>metrocluster configure node-name</code></td>
</tr>
</tbody>
</table>
| A single mirrored data aggregate         | a. From any node's prompt, change to the advanced privilege level: `set -privilege advanced`  
                                           | You need to respond with `y` when you are prompted to continue into advanced mode and you see the advanced mode prompt (`*`). |
|                                          | b. Configure the MetroCluster with the `-allow-with-one-aggregate true` parameter:  
                                           | `metrocluster configure -allow-with-one-aggregate true node-name` |
|                                          | c. Return to the admin privilege level: `set -privilege admin` |
Example

Note: The best practice is to have multiple data aggregates. If the first DR group has only one aggregate and you want to add a DR group with one aggregate, you must move the metadata volume off the single data aggregate. For more information on this procedure, see *Moving a metadata volume in MetroCluster configurations*.

The following command enables the MetroCluster configuration on all of the nodes in the DR group that contains controller_A_1:

```bash
cluster_A::*> metrocluster configure -node-name controller_A_1
```

[Job 121] Job succeeded: Configure is successful.

2. Verify the networking status on site A:

   ```bash
   network port show
   ```

Example

The following example shows the network port usage:

```
cluster_A::> network port show

<table>
<thead>
<tr>
<th>Node</th>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Speed (Mbps)</th>
<th>Admin/Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_A_1</td>
<td>e0a</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>Cluster</td>
<td>Cluster</td>
<td>up</td>
<td>9000</td>
<td>auto/1000</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td>auto/1000</td>
</tr>
<tr>
<td></td>
<td>e0g</td>
<td>Default</td>
<td>Default</td>
<td>up</td>
<td>1500</td>
<td>auto/1000</td>
<td>auto/1000</td>
</tr>
</tbody>
</table>
```

7 entries were displayed.

3. Verify the MetroCluster configuration from both sites in the MetroCluster configuration.

a. Verify the configuration from site A:

   ```bash
   metrocluster show
   ```

Example

```
cluster_A::> metrocluster show

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Entry Name</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local:</td>
<td>Configuration state</td>
<td>configured</td>
</tr>
<tr>
<td>cluster_A</td>
<td>Mode</td>
<td>normal</td>
</tr>
<tr>
<td></td>
<td>AUSO Failure Domain</td>
<td>auso-on-cluster-disaster</td>
</tr>
<tr>
<td>Remote:</td>
<td>Configuration state</td>
<td>configured</td>
</tr>
<tr>
<td>cluster_B</td>
<td>Mode</td>
<td>normal</td>
</tr>
<tr>
<td></td>
<td>AUSO Failure Domain</td>
<td>auso-on-cluster-disaster</td>
</tr>
</tbody>
</table>
```

b. Verify the configuration from site B:

   ```bash
   metrocluster show
   ```
### Configuring FC-to-SAS bridges for health monitoring

If your configuration includes FC-to-SAS bridges, you must perform some special configuration steps to monitor the FC-to-SAS bridges in the MetroCluster configuration.

#### About this task
Third-party SNMP monitoring tools are not supported for FibreBridge bridges.

#### Step

1. From the ONTAP cluster prompt, add the bridge to health monitoring:
   
   a. Add the bridge, using the command for your version of ONTAP:

<table>
<thead>
<tr>
<th>ONTAP version</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5 and later</td>
<td>storage bridge add -address 0.0.0.0 -managed-by in-band -name bridge-name</td>
</tr>
<tr>
<td>9.4 and earlier</td>
<td>storage bridge add -address bridge-ip-address -name bridge-name</td>
</tr>
</tbody>
</table>

   b. Verify that the bridge has been added and is properly configured:

   ```
   storage bridge show
   ```

   It might take as long as 15 minutes to reflect all data because of the polling interval. The ONTAP health monitor can contact and monitor the bridge if the value in the Status column is `ok`, and other information, such as the worldwide name (WWN), is displayed.

### Example

The following example shows that the FC-to-SAS bridges are configured:

```
controller_A_1::> storage bridge show
Bridge Model Symbolic Name Is Monitored Monitor Status Vendor
------------------ ------------- ------------------ --------- ------
Atto 7500N       atto01        true          ok          Atto FibreBridge
        7500N       atto02        true          ok          Atto FibreBridge
        7500N       atto03        true          ok          Atto FibreBridge
        7500N       atto04        true          ok          Atto FibreBridge
        7500N       atto05        true          ok          Atto FibreBridge
        7500N       atto06        true          ok          Atto FibreBridge
        7500N       atto07        true          ok          Atto FibreBridge
        7500N       atto08        true          ok          Atto FibreBridge
        7500N       atto09        true          ok          Atto FibreBridge
        7500N       atto10        true          ok          Atto FibreBridge
        7500N       atto11        true          ok          Atto FibreBridge
        7500N       atto12        true          ok          Atto FibreBridge
        7500N       atto13        true          ok          Atto FibreBridge
        7500N       atto14        true          ok          Atto FibreBridge
        7500N       atto15        true          ok          Atto FibreBridge
        7500N       atto16        true          ok          Atto FibreBridge
        7500N       atto17        true          ok          Atto FibreBridge
        7500N       atto18        true          ok          Atto FibreBridge
        7500N       atto19        true          ok          Atto FibreBridge
        7500N       atto20        true          ok          Atto FibreBridge
4 entries were displayed
controller_A_1::>
```
Checking the MetroCluster configuration

You can check that the components and relationships in the MetroCluster configuration are working correctly. You should do a check after initial configuration and after making any changes to the MetroCluster configuration. You should also do a check before a negotiated (planned) switchover or a switchback operation.

About this task

If the `metrocluster check run` command is issued twice within a short time on either or both clusters, a conflict can occur and the command might not collect all data. Subsequent `metrocluster check show` commands do not show the expected output.

Steps

1. Check the configuration:

   `metrocluster check run`

   **Example**

   The command runs as a background job and might not be completed immediately.

   ```
   cluster_A::> metrocluster check run
   The operation has been started and is running in the background. Wait for
   it to complete and run "metrocluster check show" to view the results. To
   check the status of the running metrocluster check operation, use the
   command, "metrocluster operation history show -job-id 2245"
   ```

   ```
   cluster_A::> metrocluster check show
   Last Checked On: 9/13/2017 20:41:37
   Component           Result
   ------------------- ---------
   nodes               ok
   lifs                ok
   config-replication  ok
   aggregates          ok
   clusters            ok
   5 entries were displayed.
   ```

2. Display more detailed results from the most recent `metrocluster check run` command:

   `metrocluster check aggregate show`
   `metrocluster check cluster show`
   `metrocluster check config-replication show`
   `metrocluster check lif show`
   `metrocluster check node show`

   The `metrocluster check show` commands show the results of the most recent `metrocluster check run` command. You should always run the `metrocluster check run` command prior to using the `metrocluster check show` commands so that the information displayed is current.
Example

The following example shows the `metrocluster check aggregate show` command output for a healthy four-node MetroCluster configuration:

```
cluster_A::> metrocluster check aggregate show
Last Checked On: 8/5/2014 00:42:58

<table>
<thead>
<tr>
<th>Node</th>
<th>Aggregate</th>
<th>Check</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>controller_A_1</td>
<td>controller_A_1_aggr0</td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_1_aggr1</td>
<td></td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_1_aggr2</td>
<td></td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_2</td>
<td>controller_A_2_aggr0</td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_2_aggr1</td>
<td></td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
<tr>
<td>controller_A_2_aggr2</td>
<td></td>
<td>mirroring-status</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>disk-pool-allocation</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ownership-state</td>
<td>ok</td>
</tr>
</tbody>
</table>
```

18 entries were displayed.

The following example shows the `metrocluster check cluster show` command output for a healthy four-node MetroCluster configuration. It indicates that the clusters are ready to perform a negotiated switchover if necessary.

```
Last Checked On: 9/13/2017 20:47:04

<table>
<thead>
<tr>
<th>Cluster</th>
<th>Check</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>mccint-fas9000-0102</td>
<td>negotiated-switchover-ready</td>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
<td>switchback-ready</td>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
<td>job-schedules</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td>licenses</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td>periodic-check-enabled</td>
<td>ok</td>
</tr>
<tr>
<td>mccint-fas9000-0304</td>
<td>negotiated-switchover-ready</td>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
<td>switchback-ready</td>
<td>not-applicable</td>
</tr>
<tr>
<td></td>
<td>job-schedules</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td>licenses</td>
<td>ok</td>
</tr>
<tr>
<td></td>
<td>periodic-check-enabled</td>
<td>ok</td>
</tr>
</tbody>
</table>
```

10 entries were displayed.

Related information

- Disk and aggregate management
- Network and LIF management
Checking for MetroCluster configuration errors with Config Advisor

You can go to the NetApp Support Site and download the Config Advisor tool to check for common configuration errors.

About this task

Config Advisor is a configuration validation and health check tool. You can deploy it at both secure sites and non-secure sites for data collection and system analysis.

Note: Support for Config Advisor is limited, and available only online.

Steps

1. Go to the Config Advisor download page and download the tool.

   NetApp Downloads: Config Advisor

2. Run Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Verifying switchover, healing, and switchback

You should verify the switchover, healing, and switchback operations of the MetroCluster configuration.

Step

1. Use the procedures for negotiated switchover, healing, and switchback that are mentioned in the MetroCluster Management and Disaster Recovery Guide.

   MetroCluster management and disaster recovery

Installing the MetroCluster Tiebreaker software

You can download and install Tiebreaker software to monitor the two clusters and the connectivity status between them from a third site. Doing so enables each partner in a cluster to distinguish between an ISL failure (when inter-site links are down) and a site failure.

Before you begin

You must have a Linux host available that has network connectivity to both clusters in the MetroCluster configuration.

Steps

1. Go to MetroCluster Tiebreaker Software Download page.

   NetApp Downloads: MetroCluster Tiebreaker for Linux

2. Follow the directions to download the Tiebreaker software and documentation.
Protecting configuration backup files

You can provide additional protection for the cluster configuration backup files by specifying a remote URL (either HTTP or FTP) where the configuration backup files will be uploaded in addition to the default locations in the local cluster.

Step

1. Set the URL of the remote destination for the configuration backup files:

   `system configuration backup settings modify URL-of-destination`

   The System Administration Guide contains additional information under the section *Managing configuration backups*.

   *System administration*

Related information

*System administration*
Testing the MetroCluster configuration

You can test failure scenarios to confirm the correct operation of the MetroCluster configuration.

Verifying negotiated switchover

You can test the negotiated (planned) switchover operation to confirm uninterrupted data availability.

About this task

This test validates that data availability is not affected (except for Microsoft Server Message Block (SMB) and Solaris Fibre Channel protocols) by switching the cluster over to the second data center.

This test should take about 30 minutes.

This procedure has the following expected results:

• The `metrocluster switchover` command will present a warning prompt.
  If you respond `yes` to the prompt, the site from where the command is issued should switch over to the partner site.

• Nodes at the partner site should shut down gracefully and remain at the LOADER> prompt.

Steps

1. Confirm that all nodes are in the configured state and normal mode:
   `metrocluster node show`

   Example

   ```
   cluster_A::> metrocluster node show
   Cluster                      Configuration State  Mode
   ----------------------------- ---------------------- ------------------------
   Local: cluster_A             configured             normal
   Remote: cluster_B            configured             normal
   ```

2. Begin the switchover operation:
   `metrocluster switchover`

   Example

   ```
   cluster_A::> metrocluster switchover
   Warning: negotiated switchover is about to start. It will stop all the data Vservers on cluster "cluster_B" and automatically re-start them on cluster "cluster_A". It will finally gracefully shutdown cluster "cluster_B".
   ```

3. Confirm that the local cluster is in the configured state and switchover mode:
   `metrocluster node show`

   Example

   ```
   cluster_A::> metrocluster node show
   Cluster                      Configuration State  Mode
   ----------------------------- ---------------------- ------------------------
   ```
4. Confirm that the switchover operation was successful:

```bash
metrocluster operation show
```

**Example**

```
cluster_A::> metrocluster operation show
```

5. Use the `vserver show` and `network interface show` commands to verify that DR SVMs and LIFs have come online.

## Verifying healing and manual switchback

You can test the healing and manual switchback operations to verify that data availability is not affected (except for SMB and Solaris FC configurations) by switching back the cluster to the original data center after a negotiated switchover.

### About this task

This test should take about 30 minutes.

The expected result of this procedure is that services should be switched back to their home nodes.

The healing steps are not required on systems running ONTAP 9.5 or later, on which healing is performed automatically after a negotiated switchover. On systems running ONTAP 9.6 and later, healing is also performed automatically after unscheduled switchover.

### Steps

1. If the system is running ONTAP 9.4 or earlier, heal the data aggregate:

   ```bash
   metrocluster heal aggregates
   ```

   **Example**

   ```
   cluster_A::> metrocluster heal aggregates
   [Job 936] Job succeeded: Heal Aggregates is successful.
   ```

2. If it is required by your configuration, heal the root aggregate:

   ```bash
   metrocluster heal root-aggregates
   ```

   **This step is required on the following configurations:**

   - MetroCluster FC configurations.
   - MetroCluster IP configurations running ONTAP 9.4 or earlier.

   **Example**

   ```
   cluster_A::> metrocluster heal root-aggregates
   ```

   The following example shows the successful completion of the command:
3. Verify that healing is completed:

```bash
cluster_A::> metrocluster heal root-aggregates
[Job 937] Job succeeded: Heal Root Aggregates is successful.
```

**Example**

The following example shows the successful completion of the command:

```bash
cluster_A::> metrocluster node show
```

<table>
<thead>
<tr>
<th>DR</th>
<th>Group</th>
<th>Cluster</th>
<th>Node</th>
<th>State</th>
<th>Mirroring Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cluster_A</td>
<td>node_A_1</td>
<td>configured</td>
<td>enabled</td>
<td>heal roots completed</td>
</tr>
<tr>
<td></td>
<td>cluster_B</td>
<td>node_B_2</td>
<td>unreachable</td>
<td>-</td>
<td>switched over</td>
</tr>
</tbody>
</table>

42 entries were displayed.

**metrocluster operation show**

If the automatic healing operation fails for any reason, you must issue the `metrocluster heal` commands manually as done in ONTAP versions prior to ONTAP 9.5. You can use the `metrocluster operation show` and `metrocluster operation history show` commands to monitor the status of healing and determine the cause of a failure.

4. Verify that all aggregates are mirrored:

```bash
cluster_A::> storage aggregate show
```

**Example**

The following example shows that all aggregates have a RAID Status of `mirrored`:

```bash
cluster_A::> storage aggregate show
```

<table>
<thead>
<tr>
<th>Cluster Aggregates:</th>
<th>Aggregate Size</th>
<th>Available</th>
<th>Used%</th>
<th>State</th>
<th>#Vols</th>
<th>Nodes</th>
<th>RAID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>data_cluster</td>
<td>4.19TB</td>
<td>4.13TB</td>
<td>2%</td>
<td>online</td>
<td>8</td>
<td>node_A_1</td>
<td>raid_dp, mirrored, normal</td>
</tr>
<tr>
<td>root_cluster</td>
<td>715.5GB</td>
<td>212.7GB</td>
<td>70%</td>
<td>online</td>
<td>1</td>
<td>node_A_1</td>
<td>raid4, mirrored, normal</td>
</tr>
</tbody>
</table>

**cluster_B Switched Over Aggregates:**

<table>
<thead>
<tr>
<th>Aggregate Size</th>
<th>Available</th>
<th>Used%</th>
<th>State</th>
<th>#Vols</th>
<th>Nodes</th>
<th>RAID Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>data_cluster_B</td>
<td>4.19TB</td>
<td>4.11TB</td>
<td>2%</td>
<td>online</td>
<td>5</td>
<td>node_A_1</td>
</tr>
<tr>
<td>root_cluster_B</td>
<td>-</td>
<td>-</td>
<td>unknown</td>
<td>-</td>
<td>-</td>
<td>node_A_1</td>
</tr>
</tbody>
</table>

5. Boot nodes from the disaster site.

6. Check the status of switchback recovery:

```bash
cluster_A::> metrocluster node show
```

**Example**

```bash
cluster_A::> metrocluster node show
```

<table>
<thead>
<tr>
<th>DR</th>
<th>Group</th>
<th>Cluster</th>
<th>Node</th>
<th>Configuration</th>
<th>State</th>
<th>Mirroring Mode</th>
<th>Mirroring Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>cluster_A</td>
<td>node_A_1</td>
<td></td>
<td>configured</td>
<td>enabled</td>
<td>heal roots completed</td>
<td></td>
</tr>
</tbody>
</table>

completed
7. Perform the switchback:

```
metrocluster switchback
```

Example

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful. Verify switchback
```

8. Confirm status of the nodes:

```
metrocluster node show
```

Example

```
cluster_A::> metrocluster node show
DR Group Cluster Node               Configuration  DR
              State          Mirroring Mode
-----------------  --------------  ----------
1     cluster_A
       node_A_1         configured     enabled   normal
       cluster_B
       node_B_2         configured     enabled   normal
2 entries were displayed.
```

9. Confirm status of the metrocluster operation:

```
metrocluster operation show
```

Example

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: 2/6/2016 13:54:25
End Time: 2/6/2016 13:56:15
Errors: -
```

Loss of a single FC-to-SAS bridge

You can test the failure of a single FC-to-SAS bridge to make sure there is no single point of failure.

About this task

This test should take about 15 minutes.

This procedure has the following expected results:

- Errors should be generated as the bridge is switched off.
- No failover or loss of service should occur.
• Only one path from the controller module to the drives behind the bridge is available.

Steps
1. Turn off the power supplies of the bridge.
2. Confirm that the bridge monitoring indicates an error:

   storage bridge show

Example

```
cluster_A::> storage bridge show
Bridge Symbolic Name Vendor Model Bridge WWN Is Monitored Status
---------- ------------- ------- --------- ----------------- -------- -------
ATTO_10.65.57.145 bridge_A_1 Atto FibreBridge 6500N 200000108662d46c true error
```

3. Confirm that drives behind the bridge are available with a single path:

   storage disk error show

Example

```
cluster_A::> storage disk error show
Disk Error Type Error Text
---------- --------- ---------------------------------------------------------------
1.0.0 onedomain 1.0.0 (5000cca057729118): All paths to this array LUN are connected to the same fault domain. This is a single point of failure.
1.0.1 onedomain 1.0.1 (5000cca057727364): All paths to this array LUN are connected to the same fault domain. This is a single point of failure.
1.0.2 onedomain 1.0.2 (5000cca05772e9d4): All paths to this array LUN are connected to the same fault domain. This is a single point of failure.
... 1.0.23 onedomain 1.0.23 (5000cca05772e9d4): All paths to this array LUN are connected to the same fault domain. This is a single point of failure.
```

Verifying operation after power line disruption

You can test the MetroCluster configuration's response to the failure of a PDU.

About this task

The best practice is for each power supply unit (PSU) in a component to be connected to separate power supplies. If both PSUs are connected to the same power distribution unit (PDU) and an electrical disruption occurs, the site could down or a complete shelf might become unavailable. Failure of one power line is tested to confirm that there is no cabling mismatch that could cause a service disruption.

This test should take about 15 minutes.

This test requires turning off power to all left-hand PDUs and then all right-hand PDUs on all of the racks containing the MetroCluster components.

This procedure has the following expected results:

• Errors should be generated as the bridge is switched off.
• No failover or loss of service should occur.
• Only one path from the controller module to the drives behind the bridge is available.
Steps

1. Turn off the power of the PDUs on the left-hand side of the rack containing the MetroCluster components.

2. Monitor the result on the console by using the `system environment sensors show -state fault` and `storage shelf show -errors` commands.

Example

```
cluster_A::> system environment sensors show -state fault

----------------- --------------- ---------- ---------- ----------
node_A_1
  PSU1           fault          PSU_OFF
  PSU1 Pwr In OK faul t          PSU OFF
node_A_2
  PSU1           fault          PSU OFF
  PSU1 Pwr In OK faul t          PSU OFF

4 entries were displayed.
```

```
cluster_A::> storage shelf show -errors

Shelf Name: 1.1
Shelf UID: 50:0a:09:80:03:6c:44:d5
Serial Number: SHFHU1443000059

Error Type          Description
------------------  ---------------------------
Power               Critical condition is detected in storage shelf power supply unit "1". The unit might fail. Reconnect PSU1
```

3. Turn the power back on to the left-hand PDUs.

4. Make sure that ONTAP clears the error condition.

5. Repeat the previous steps with the right-hand PDUs.

Verifying operation after loss of a single storage shelf

You can test the failure of a single storage shelf to verify that there is no single point of failure.

About this task

This procedure has the following expected results:

- An error message should be reported by the monitoring software.
- No failover or loss of service should occur.
- Mirror resynchronization starts automatically after the hardware failure is restored.

Steps

1. Check the storage failover status:

   `storage failover show`
Example

```
Example

cluster_A::> storage failover show

Node           Partner        Possible State Description
-------------- -------------- --------
-------------- -------------- --------
node_A_1       node_A_2       true     Connected to node_A_2
node_A_2       node_A_1       true     Connected to node_A_1

2 entries were displayed.
```

2. Check the aggregate status:

```
storage aggregate show
```

Example

```
Example

cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID Status
--------- -------- --------- ----- ------- ------ ---------------- ------------
node_A_1data01_mirrored
4.15TB    3.40TB   18% online       3 node_A_1       raid_dp, mirrored, normal
node_A_1root
707.7GB   34.29GB   95% online       1 node_A_1       raid_dp, mirrored, normal
node_A_2_data01_mirrored
4.15TB    4.12TB    1% online       2 node_A_2       raid_dp, mirrored, normal
node_A_2_data02_unmirrored
2.18TB    2.18TB    0% online       1 node_A_2       raid_dp, normal
node_A_2_root
707.7GB   34.27GB   95% online       1 node_A_2       raid_dp, mirrored, normal
```

3. Verify that all data SVMs and data volumes are online and serving data:

```
vserver show -type data
network interface show -fields is-home false
volume show !vol0,!MDV*
```

Example

```
Example

cluster_A::> vserver show -type data

cluster_A::> vserver show -type data

Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
SVM1
SVM1_root
node_A_1data01_mirrored
online     RW         10GB     9.50GB    5%
node_A_2data01_mirrored
3.40TB   3.40TB   18% online       3 node_A_1       raid_dp, mirrored, normal
node_A_2_data02_unmirrored
2.18TB    2.18TB    0% online       1 node_A_2       raid_dp, normal
node_A_2_root
707.7GB   34.27GB   95% online       1 node_A_2       raid_dp, mirrored, normal
```
4. Identify a shelf in Pool 1 for node node_A_2 to power off to simulate a sudden hardware failure:  
   `storage aggregate show -r -node node-name !*root`

   The shelf you select must contain drives that are part of a mirrored data aggregate.

   **Example**

   In the following example, shelf ID 31 is selected to fail.

   ```
   cluster_A::> storage aggregate show -r -node node_A_2 !*root
   Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block checksums)
   Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block checksums)

   Position Disk Pool Type RPM Size Size Status
    -------- --------------------------- ---- ----- ------ -------- -------- ----------
    dparity  2.30.3                       0   BSAS    7200  827.7GB  828.0GB (normal)
    parity   2.30.4                       0   BSAS    7200  827.7GB  828.0GB (normal)
    data     2.30.6                       0   BSAS    7200  827.7GB  828.0GB (normal)
    data     2.30.8                       0   BSAS    7200  827.7GB  828.0GB (normal)
    data     2.30.5                       0   BSAS    7200  827.7GB  828.0GB (normal)
   Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block checksums)

   Position Disk Pool Type RPM Size Size Status
    -------- --------------------------- ---- ----- ------ -------- -------- ----------
    dparity  1.31.7                       1   BSAS    7200  827.7GB  828.0GB (normal)
    parity   1.31.6                       1   BSAS    7200  827.7GB  828.0GB (normal)
    data     1.31.3                       1   BSAS    7200  827.7GB  828.0GB (normal)
    data     1.31.4                       1   BSAS    7200  827.7GB  828.0GB (normal)
    data     1.31.5                       1   BSAS    7200  827.7GB  828.0GB (normal)
   15 entries were displayed.
   ```

5. Physically power off the shelf that you selected.

6. Check the aggregate status again:

   ```
   storage aggregate show
   storage aggregate show -r -node node_A_2 !*root
   ```

   **Example**

   The aggregate with drives on the powered-off shelf should have a degraded RAID status, and drives on the affected plex should have a failed status, as shown in the following example:

   ```
   cluster_A::> storage aggregate show
   Aggregate Size Available Used% State #Vols Nodes RAID Status
   -------- ------ --------- ----- ------ ---------- ---------------
   node_A_1data01_mirrored 4.15TB 3.40TB 18% online 3 node_A_1 raid_dp, mirrored, normal
   node_A_1root 707.7GB 34.29GB 95% online 1 node_A_1 raid_dp, mirrored, normal
   node_A_2_data01_mirrored 4.15TB 4.12TB 1% online 2 node_A_2 raid_dp,
   ```
7. Verify that the data is being served and that all volumes are still online:

```
vserver show -type data
network interface show -fields is-home false
volume show !vol0,!MDV*
```

Example

```
cluster_A::> vserver show -type data

Vserver Type        Subtype State    Operational Root Aggregate
----------- ------- ---------- --------- ------------ ----------- -------------
SVM1        data    sync-source running node_A_1_data01_mirrored/SVM1_root node_A_1_data01_mirrored
SVM2        data    sync-source running node_A_1_data01_mirrored/SVM2_root

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*

Vserver Volume Aggregate State Type  Size      Available  Used%  
----------- ----------- --------- ---------- ----------- ----------- -----------
SVM1        node_A_1data01_mirrored online RW    10GB       9.50GB     5%
SVM1        node_A_1data01_mirrored online RW    10GB       9.49GB     5%
SVM2        node_A_1data01_mirrored online RW    10GB       9.49GB     5%
```
8. Physically power on the shelf.
   Resynchronization starts automatically.

9. Verify that resynchronization has started:

   ```
   storage aggregate show
   ```

   **Example**

   The affected aggregate should have a **resyncing** RAID status, as shown in the following example:

   ```
   cluster_A::> storage aggregate show
   cluster Aggregates:
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID Status
   --------- -------- --------- ----- ------- ------ ---------------- ------------
   node_A_1_data01_mirrored 4.15TB   3.40TB  18% online       3 node_A_1       raid_dp, mirrored, normal
   node_A_1_root             707.7GB   34.29GB  95% online       1 node_A_1       raid_dp, mirrored, normal
   node_A_2_data01_mirrored 4.15TB   4.12TB  1% online       2 node_A_2       raid_dp, resyncing
   node_A_2_data02_unmirrored 2.18TB   2.18TB  0% online       1 node_A_2       raid_dp, normal
   node_A_2_root             707.7GB   34.27GB  95% online       1 node_A_2       raid_dp, resyncing
   ```

10. Monitor the aggregate to confirm that resynchronization is complete:

    ```
    storage aggregate show
    ```

    **Example**

    The affected aggregate should have a **normal** RAID status, as shown in the following example:

    ```
    cluster_A::> storage aggregate show
    cluster Aggregates:
    Aggregate     Size Available Used% State   #Vols  Nodes            RAID Status
    --------- -------- --------- ----- ------- ------ ---------------- ------------
    node_A_1_data01_mirrored 4.15TB   3.40TB  18% online       3 node_A_1       raid_dp, mirrored, normal
    node_A_1_root             707.7GB   34.29GB  95% online       1 node_A_1       raid_dp, mirrored, normal
    node_A_2_data01_mirrored 4.15TB   4.12TB  1% online       2 node_A_2       raid_dp, normal
    node_A_2_data02_unmirrored 2.18TB   2.18TB  0% online       1 node_A_2       raid_dp, normal
    node_A_2_root             707.7GB   34.27GB  95% online       1 node_A_2       raid_dp, resyncing
    ```
Connections in a stretch MetroCluster configurations with array LUNs

In a stretch MetroCluster configuration with array LUNs, you must connect the FC-VI ports across controllers. Direct connectivity is supported between the controllers and E-Series storage arrays. For all other array LUN configurations, you must use FC switches in the configuration.

You can also set up a stretch MetroCluster configuration with both disks and array LUNs. In such a configuration, you must use either FC-to-SAS bridges or SAS optical cables to connect the controllers to disks.

Example of a stretch MetroCluster configuration with array LUNs

In a stretch MetroCluster configuration with array LUNs, you must cable the FC-VI ports for direct connectivity between the controllers. In addition, you must cable each controller’s HBA ports to switch ports on the corresponding FC switches. Cabling to the array LUNs is the same as that in a fabric-attached MetroCluster, except for E-Series array LUNs, which can be directly connected.

The following illustration shows the FC-VI ports cabled across controllers A and B in a stretch MetroCluster configuration:

```
+----------------+                  +----------------+                  +----------------+
| Site A          | Site B                  | Site C          |
| Controller A    | Controller B            | Controller C    |
| FC - VI a       | FC - VI b               | FC - VI a       |
| FC - VI a       | FC - VI b               | FC - VI a       |
|                 |                         |                 |
```

Note: FAS9000 storage systems controller modules use four FC-VI ports each.

For configurations with E-Series array LUNs, you can directly attach the E-Series LUNs.

NetApp Knowledgebase Answer 1001397: FAQ: Direct Attach support for Stretch MetroCluster Configuration with NetApp E-Series array

Except for connecting the FC-VI ports, the rest of the procedure for setting up a MetroCluster configuration with array LUNs that are not using E-Series array LUNs requires FC switches and is the same as using array LUNs in fabric-attached configurations.

Fabric-attached MetroCluster installation and configuration

Examples of two-node stretch MetroCluster configurations with disks and array LUNs

For setting up a stretch MetroCluster configuration with native disks and array LUNs, you must use either FC-to-SAS bridges or SAS optical cables to connect the ONTAP systems to the disk shelves. You must use FC switches for connecting array LUNs to the ONTAP systems.

A minimum of eight HBA ports is required for an ONTAP system to connect to both native disks and array LUNs.
In the following examples representing two-node stretch MetroCluster configurations with disks and array LUNs, HBA ports 0a through 0d are used for connection with array LUNs, while ports 1a through 1d are used for connections with native disks.

The following illustration shows a two-node stretch MetroCluster configuration in which the native disks are connected to the ONTAP systems through *SAS optical cables*:

The following illustration shows a two-node stretch MetroCluster configuration in which the native disks are connected to the ONTAP systems through *FC-to-SAS bridges*:

The following illustration shows a two-node stretch MetroCluster configuration with the array LUN connections:
Note: If required, you can also use the same FC switches to connect both native disks and array LUNs to the controllers in the MetroCluster configuration.

**Fabric-attached MetroCluster installation and configuration**

**Example of a stretch MetroCluster configuration with E-Series storage arrays**

In a stretch MetroCluster configuration with E-Series storage array LUNs, you can directly connect the storage controllers and the storage arrays. Unlike other array LUNs, FC switches are not required.

The *Direct Attach support for Stretch MetroCluster Configuration with NetApp E-Series array* KnowledgeBase article provides examples of configurations with E-Series array LUNs.

*NetApp Knowledgebase Answer 1001397: FAQ: Direct Attach support for Stretch MetroCluster Configuration with NetApp E-Series array*
Considerations when removing MetroCluster configurations

You can remove the MetroCluster configuration from all of the nodes in a disaster recovery (DR) group. After removing the MetroCluster configuration, all disk connectivity and interconnects should be adjusted to be in a supported state. If you need to remove the MetroCluster configuration, contact technical support.

**Attention:** You cannot reverse the MetroCluster unconfiguration. This process should only be done with the assistance of technical support.
Using the Active IQ Unified Manager and ONTAP System Manager for further configuration and monitoring

The Active IQ Unified Manager and ONTAP System Manager can be used for GUI management of the clusters and monitoring of the configuration.

Each node has ONTAP System Manager pre-installed. To load System Manager, enter the cluster management LIF address as the URL in a web browser that has connectivity to the node.

You can also use Active IQ Unified Manager to monitor the MetroCluster configuration.

Related information

Active IQ Unified Manager and ONTAP System Manager Documentation

Synchronizing the system time using NTP

Each cluster needs its own Network Time Protocol (NTP) server to synchronize the time between the nodes and their clients. You can use the Edit DateTime dialog box in System Manager to configure the NTP server.

Before you begin

You must have downloaded and installed System Manager. System Manager is available from the NetApp Support Site.

About this task

• You cannot modify the time zone settings for a failed node or the partner node after a takeover occurs.

• Each cluster in the MetroCluster FC configuration should have its own separate NTP server or servers used by the nodes and (if present) FC-to-SAS bridges at that MetroCluster site.

  If you are using the MetroCluster Tiebreaker software, it should also have its own separate NTP server.

Steps

1. From the home page, double-click the appropriate storage system.

2. Expand the Cluster hierarchy in the left navigation pane.

3. In the navigation pane, click Configuration > System Tools > DateTime.

4. Click Edit.

5. Select the time zone.

6. Specify the IP addresses of the time servers, and then click Add.

   You must add an NTP server to the list of time servers. The domain controller can be an authoritative server.

7. Click OK.

8. Verify the changes you made to the date and time settings in the Date and Time window.
Considerations when using ONTAP in a MetroCluster configuration

When using ONTAP in a MetroCluster configuration, you should be aware of certain considerations for licensing, peering to clusters outside the MetroCluster configuration, performing volume operations, NVFAIL operations, and other ONTAP operations.

Licensing considerations
• Both sites should be licensed for the same site-licensed features.
• All nodes should be licensed for the same node-locked features.

SnapMirror consideration
• SnapMirror SVM disaster recovery is only supported on MetroCluster configurations running versions of ONTAP 9.5 or later.

FlexGroup support in MetroCluster configurations
Starting with ONTAP 9.6 MetroCluster configurations support FlexGroup volumes.

Job schedules in a MetroCluster configuration
In ONTAP 9.3 and later, user-created job schedules are automatically replicated between clusters in a MetroCluster configuration. If you create, modify, or delete a job schedule on a cluster, the same schedule is automatically created on the partner cluster, using Configuration Replication Service (CRS).

Note: System-created schedules are not replicated and you must manually perform the same operation on the partner cluster so that job schedules on both clusters are identical.

Cluster peering from the MetroCluster site to a third cluster
Because the peering configuration is not replicated, if you peer one of the clusters in the MetroCluster configuration to a third cluster outside of that configuration, you must also configure the peering on the partner MetroCluster cluster. This is so that peering can be maintained if a switchover occurs.

The non-MetroCluster cluster must be running ONTAP 8.3 or later. If not, peering is lost if a switchover occurs even if the peering has been configured on both MetroCluster partners.

LDAP client configuration replication in a MetroCluster configuration
An LDAP client configuration created on a storage virtual machine (SVM) on a local cluster is replicated to its partner data SVM on the remote cluster. For example, if the LDAP client configuration is created on the admin SVM on the local cluster, then it is replicated to all the admin data SVMs on the remote cluster. This MetroCluster feature is intentional so that the LDAP client configuration is active on all the partner SVMs on the remote cluster.
Networking and LIF creation guidelines for MetroCluster configurations

You should be aware of how LIFs are created and replicated in a MetroCluster configuration. You must also know about the requirement for consistency so that you can make proper decisions when configuring your network.

Related information

ONTAP concepts

IPspace object replication and subnet configuration requirements

You should be aware of the requirements for replicating IPspace objects to the partner cluster and for configuring subnets and IPv6 in a MetroCluster configuration.

IPspace replication

You must consider the following guidelines while replicating IPspace objects to the partner cluster:

- The IPspace names of the two sites must match.
- IPspace objects must be manually replicated to the partner cluster.
  Any storage virtual machines (SVMs) that are created and assigned to an IPspace before the IPspace is replicated will not be replicated to the partner cluster.

Subnet configuration

You must consider the following guidelines while configuring subnets in a MetroCluster configuration:

- Both clusters of the MetroCluster configuration must have a subnet in the same IPspace with the same subnet name, subnet, broadcast domain, and gateway.
- The IP ranges of the two clusters must be different.

In the following example, the IP ranges are different:

```
cluster_A::> network subnet show
IPspace: Default
Subnet Name Subnet Broadcast Domain Gateway Avail/ Total Ranges
--------- ---- --------- ----------- ----------- -------
subnet1 192.168.2.0/24 Default 192.168.2.1 10/10
192.168.2.11-192.168.2.20
cluster_B::> network subnet show
IPspace: Default
Subnet Name Subnet Broadcast Domain Gateway Avail/ Total Ranges
--------- ---- --------- ----------- ----------- -------
subnet1 192.168.2.0/24 Default 192.168.2.1 10/10
192.168.2.21-192.168.2.30
```

IPv6 configuration

If IPv6 is configured on one site, IPv6 must be configured on the other site as well.
Requirements for LIF creation in a MetroCluster configuration

You should be aware of the requirements for creating LIFs when configuring your network in a MetroCluster configuration.

You must consider the following guidelines when creating LIFs:

- Fibre Channel: You must use stretched VSAN or stretched fabrics
- IP/iSCSI: You must use layer 2 stretched network
- ARP broadcasts: You must enable ARP broadcasts between the two clusters
- Duplicate LIFs: You must not create multiple LIFs with the same IP address (duplicate LIFs) in an IPspace

Verify LIF creation

You can confirm the successful creation of a LIF in a MetroCluster configuration by running the `metrocluster check lif show` command. If you encounter any issues while creating the LIF, you can use the `metrocluster check lif repair-placement` command to fix the issues.

LIF replication and placement requirements and issues

You should be aware of the LIF replication requirements in a MetroCluster configuration. You should also know how a replicated LIF is placed on a partner cluster, and you should be aware of the issues that occur when LIF replication or LIF placement fails.

Replication of LIFs to the partner cluster

When you create a LIF on a cluster in a MetroCluster configuration, the LIF is replicated on the partner cluster. LIFs are not placed on a one-to-one name basis. For availability of LIFs after a switchover operation, the LIF placement process verifies that the ports are able to host the LIF based on reachability and port attribute checks.

The system must meet the following conditions to place the replicated LIFs on the partner cluster:

<table>
<thead>
<tr>
<th>Condition</th>
<th>LIF type: FC</th>
<th>LIF type: IP/iSCSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node identification</td>
<td>ONTAP attempts to place the replicated LIF on the disaster recovery (DR) partner of the node on which it was created. If the DR partner is unavailable, the DR auxiliary partner is used for placement.</td>
<td>ONTAP attempts to place the replicated LIF on the DR partner of the node on which it was created. If the DR partner is unavailable, the DR auxiliary partner is used for placement.</td>
</tr>
<tr>
<td>Condition</td>
<td>LIF type: FC</td>
<td>LIF type: IP/iSCSI</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port identification</td>
<td>ONTAP identifies the connected FC target ports on the DR cluster.</td>
<td>The ports on the DR cluster that are in the same IP space as the source LIF are selected for a reachability check.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If there are no ports in the DR cluster in the same IP space, the LIF cannot be placed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All of the ports in the DR cluster that are already hosting a LIF in the same IP space and subnet are automatically marked as reachable; and can be used for placement. These ports are not included in the reachability check.</td>
</tr>
<tr>
<td>Reachability check</td>
<td>Reachability is determined by checking for the connectivity of the source fabric WWN on the ports in the DR cluster. If the same fabric is not present at the DR site, the LIF is placed on a random port on the DR partner.</td>
<td>Reachability is determined by the response to an Address Resolution Protocol (ARP) broadcast from each previously identified port on the DR cluster to the source IP address of the LIF to be placed. For reachability checks to succeed, ARP broadcasts must be allowed between the two clusters. Each port that receives a response from the source LIF will be marked as possible for placement.</td>
</tr>
</tbody>
</table>
Considerations when using ONTAP in a MetroCluster configuration

<table>
<thead>
<tr>
<th>Condition</th>
<th>LIF type: FC</th>
<th>LIF type: IP/iSCSI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port selection</td>
<td>ONTAP categorizes the ports based on attributes such as adapter type and speed, and then selects the ports with matching attributes. If no ports with matching attributes are found, the LIF is placed on a random connected port on the DR partner.</td>
<td>From the ports that are marked as reachable during the reachability check, ONTAP prefers ports that are in the broadcast domain that is associated with the subnet of the LIF. If there are no network ports available on the DR cluster that are in the broadcast domain that is associated with the subnet of the LIF, then ONTAP selects ports that have reachability to the source LIF. If there are no ports with reachability to the source LIF, a port is selected from the broadcast domain that is associated with the subnet of the source LIF, and if no such broadcast domain exists, a random port is selected. ONTAP categorizes the ports based on attributes such as adapter type, interface type, and speed, and then selects the ports with matching attributes.</td>
</tr>
<tr>
<td>LIF placement</td>
<td>From the reachable ports, ONTAP selects the least loaded port for placement.</td>
<td>From the selected ports, ONTAP selects the least loaded port for placement.</td>
</tr>
</tbody>
</table>

**Placement of replicated LIFs when the DR partner node is down**

When an iSCSI or FC LIF is created on a node whose DR partner has been taken over, the replicated LIF is placed on the DR auxiliary partner node. After a subsequent giveback operation, the LIFs are not automatically moved to the DR partner. This can lead to LIFs being concentrated on a single node in the partner cluster. During a MetroCluster switchover operation, subsequent attempts to map LUNs belonging to the storage virtual machine (SVM) fail.

You should run the `metrocluster check lif show` command after a takeover operation or giveback operation to verify that the LIF placement is correct. If errors exist, you can run the `metrocluster check lif repair-placement` command to resolve the issues.

**LIF placement errors**

LIF placement errors that are displayed by the `metrocluster check lif show` command are retained after a switchover operation. If the `network interface modify`, `network interface rename`, or `network interface delete` command is issued for a LIF with a placement error, the error is removed and does not appear in the output of the `metrocluster check lif show` command.
LIF replication failure

You can also check whether LIF replication was successful by using the `metrocluster check lif show` command. An EMS message is displayed if LIF replication fails.

You can correct a replication failure by running the `metrocluster check lif repair-placement` command for any LIF that fails to find a correct port. You should resolve any LIF replication failures as soon as possible to verify the availability of LIF during a MetroCluster switchover operation.

**Note:** Even if the source SVM is down, LIF placement might proceed normally if there is a LIF belonging to a different SVM in a port with the same IPspace and network in the destination SVM.

Volume creation on a root aggregate

The system does not allow the creation of new volumes on the root aggregate (an aggregate with an HA policy of `CFO`) of a node in a MetroCluster configuration.

Because of this restriction, root aggregates cannot be added to an SVM using the `vserver add-aggregates` command.

SVM disaster recovery in a MetroCluster configuration

Starting with ONTAP 9.5, active storage virtual machines (SVMs) in a MetroCluster configuration can be used as sources with the SnapMirror SVM disaster recovery feature. The destination SVM must be on the third cluster outside of the MetroCluster configuration.

You should be aware of the following requirements and limitations of using SVMs with SnapMirror disaster recovery:

- Only an active SVM within a MetroCluster configuration can be the source of an SVM disaster recovery relationship.
  A source can be a sync-source SVM before switchover or a sync-destination SVM after switchover.

- When a MetroCluster configuration is in a steady state, the MetroCluster sync-destination SVM cannot be the source of an SVM disaster recovery relationship, since the volumes are not online.

The following image shows the SVM disaster recovery behavior in a steady state:
• When the sync-source SVM is the source of an SVM DR relationship, the source SVM DR relationship information is replicated to the MetroCluster partner. This enables the SVM DR updates to continue after a switchover as shown in the following image:

![MetroCluster configuration diagram](image)

• During the switchover and switchback processes, replication to the SVM DR destination might fail. However, after the switchover or switchback process completes, the next SVM DR scheduled updates will succeed.

See the section “Replicating the SVM configuration” in the Data Protection Power Guide for details on configuring an SVM DR relationship.

**Data protection**

**SVM resynchronization at a disaster recovery site**

During resynchronization, the storage virtual machines (SVMs) disaster recovery (DR) source on the MetroCluster configuration is restored from the destination SVM on the non-MetroCluster site.

During resynchronization, the source SVM (cluster_A) temporarily acts as a destination SVM as shown in the following image:
If an unplanned switchover occurs during resynchronization

Unplanned switchovers that occur during the resynchronization will halt the resynchronization transfer. If an unplanned switchover occurs, the following conditions are true:

- The destination SVM on the MetroCluster site (which was a source SVM prior to resynchronization) remains as a destination SVM. The SVM at the partner cluster will continue to retain its subtype and remain inactive.
- The SnapMirror relationship must be re-created manually with the sync-destination SVM as the destination.
- The SnapMirror relationship does not appear in the SnapMirror show output after a switchover at the survivor site unless a SnapMirror create operation is executed.

Performing switchback after an unplanned switchover during resynchronization

To successfully perform the switchback process, the resynchronization relationship must be broken and deleted. Switchback is not permitted if there are any SnapMirror DR destination SVMs in the MetroCluster configuration or if the cluster has an SVM of subtype “dp-destination”.

Output of the storage disk show and storage shelf show commands in a two-node stretch MetroCluster configuration

In a two-node stretch MetroCluster configuration, the is-local-attach field of the storage disk show and storage shelf show commands shows all of the disks and storage shelves as local, regardless of the node to which they are attached.

Output for the storage aggregate plex show command is indeterminate after a MetroCluster switchover

When you run the storage aggregate plex show command after a MetroCluster switchover, the status of plex0 of the switched over root aggregate is indeterminate and is displayed as failed.
During this time, the switched over root is not updated. The actual status of this plex can only be determined after the MetroCluster healing phase.

### Modifying volumes to set the NVFAIL flag in case of switchover

You can modify a volume so that the NVFAIL flag is set on the volume in the event of a MetroCluster switchover. The NVFAIL flag causes the volume to be fenced off from any modification. This is required for volumes that need to be handled as if committed writes to the volume were lost after the switchover.

**About this task**

**Note:** In ONTAP versions earlier than 9.0, the NVFAIL flag is used for each switchover. In ONTAP 9.0 and later versions, the unplanned switchover (USO) is used.

**Step**

1. Enable MetroCluster configuration to trigger NVFAIL on switchover by setting the `vol -dr-force-nvfail` parameter to `on`:

   ```
   vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
   ```

### Monitoring and protecting the file system consistency using NVFAIL

The `-nvfail` parameter of the `volume modify` command enables ONTAP to detect nonvolatile RAM (NVRAM) inconsistencies when the system is booting or after a switchover operation. It also warns you and protects the system against data access and modification until the volume can be manually recovered.

If ONTAP detects any problems, database or file system instances stop responding or shut down. ONTAP then sends error messages to the console to alert you to check the state of the database or file system. You can enable NVFAIL to warn database administrators of NVRAM inconsistencies among clustered nodes that can compromise database validity.

After the NVRAM data loss during failover or boot recovery, NFS clients cannot access data from any of the nodes until the NVFAIL state is cleared. CIFS clients are unaffected.

#### How NVFAIL impacts access to NFS volumes or LUNs

The NVFAIL state is set when ONTAP detects NVRAM errors when booting, when a MetroCluster switchover operation occurs, or during an HA takeover operation if the NVFAIL option is set on the volume. If no errors are detected at startup, the file service is started normally. However, if NVRAM errors are detected or NVFAIL processing is enforced on a disaster switchover, ONTAP stops database instances from responding.

When you enable the NVFAIL option, one of the processes described in the following table takes place during bootup:

<table>
<thead>
<tr>
<th>If...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONTAP detects no NVRAM errors</td>
<td>File service starts normally.</td>
</tr>
</tbody>
</table>
If... | Then...
---|---
ONTAP detects NVRAM errors | • ONTAP returns a stale file handle (\texttt{ESTALE}) error to NFS clients trying to access the database, causing the application to stop responding, crash, or shut down. ONTAP then sends an error message to the system console and log file.
• When the application restarts, files are available to CIFS clients even if you have not verified that they are valid. For NFS clients, files remain inaccessible until you reset the \texttt{in-nvfailed-state} option on the affected volume.

If one of the following parameters is used: | You can unset the \texttt{dr-force-nvfail} option after the switchover, if the administrator is not expecting to force NVFAIL processing for possible future disaster switchover operations. For NFS clients, files remain inaccessible until you reset the \texttt{in-nvfailed-state} option on the affected volume.
• \texttt{dr-force-nvfail} volume option is set
• \texttt{force-nvfail-all} switchover command option is set.

Note: Using the \texttt{force-nvfail-all} option causes the \texttt{dr-force-nvfail} option to be set on all of the DR volumes processed during the disaster switchover.

ONTAP detects NVRAM errors on a volume that contains LUNs | LUNs in that volume are brought offline. The \texttt{in-nvfailed-state} option on the volume must be cleared, and the \texttt{NVFAIL} attribute on the LUNs must be cleared by bringing each LUN in the affected volume online.
You can perform the steps to check the integrity of the LUNs and recover the LUN from a Snapshot copy or back up as necessary. After all of the LUNs in the volume are recovered, the \texttt{in-nvfailed-state} option on the affected volume is cleared.

## Commands for monitoring data loss events

If you enable the \texttt{NVFAIL} option, you receive notification when a system crash caused by NVRAM inconsistencies or a MetroCluster switchover occurs.

By default, the NVFAIL parameter is not enabled.

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new volume with NVFAIL enabled</td>
<td>\texttt{volume create -nvfail on}</td>
</tr>
<tr>
<td>Enable NVFAIL on an existing volume</td>
<td>\texttt{volume modify}</td>
</tr>
</tbody>
</table>
If you want to... | Use this command...
---|---
Display whether NVFAIL is currently enabled for a specified volume | `volume show`  
*Note: You set the `fields` parameter to `nvfail` to display the NVFAIL attribute for a specified volume.*

See the man page for each command for more information.

**Accessing volumes in NVFAIL state after a switchover**

After a switchover, you must clear the NVFAIL state by resetting the `-in-nvfailed-state` parameter of the `volume modify` command to remove the restriction of clients to access data.

**Before you begin**

The database or file system must not be running or trying to access the affected volume.

**About this task**

Setting `-in-nvfailed-state` parameter requires advanced-level privilege.

**Step**

1. Recover the volume by using the `volume modify` command with the `-in-nvfailed-state` parameter set to `false`.

**After you finish**

For instructions about examining database file validity, see the documentation for your specific database software.

If your database uses LUNs, review the steps to make the LUNs accessible to the host after an NVRAM failure.

**Recovering LUNs in NVFAIL states after switchover**

After a switchover, the host no longer has access to data on the LUNs that are in NVFAIL states. You must perform a number of actions before the database has access to the LUNs.

**Before you begin**

The database must not be running.

**Steps**

1. Clear the NVFAIL state on the affect volume that hosts the LUNs by resetting the `-in-nvfailed-state` parameter of the `volume modify` command.

2. Bring the affected LUNs online.

3. Examine the LUNs for any data inconsistencies and resolve them.
   
   This might involve host-based recovery or recovery done on the storage controller using SnapRestore.

4. Bring the database application online after recovering the LUNs.
Transitioning from a stretch to a fabric-attached MetroCluster configuration

In a fabric-attached MetroCluster configuration, the nodes are in different locations. This geographical difference increases the disaster protection. To transition from a stretch to a fabric-attached MetroCluster configuration, you must add FC switches and, if necessary, FC-to-SAS bridges to the configuration.

Before you begin

- You must have disabled automatic switchover on both of the clusters by running the `metrocluster modify -auto-switchover-failure-domain auto-disabled` command.
- You must have shut down the nodes.
  
  This procedure is disruptive.

About this task

The MetroCluster configuration must be transitioned on both sites. After upgrading the MetroCluster configuration, you must enable automatic switchover on both the clusters. You also must validate the configuration by running the `metrocluster check run` command.

This procedure gives an overview of the required steps. For detailed steps, you must refer to specific sections in the Fabric-attached MetroCluster Installation and Configuration Guide. You do not need to do a full installation and configuration.

**Fabric-attached MetroCluster installation and configuration**

**Steps**

1. Prepare for the upgrade by carefully reviewing the "Preparing for the MetroCluster installation" section of the Fabric-attached MetroCluster Installation and Configuration Guide.

2. Install, cable, and configure the required switches and FC-to-SAS bridges.
   
   **Note:** You should use the procedures in the section "Cabling a fabric-attached MetroCluster configuration" of the Fabric-attached MetroCluster Installation and Configuration Guide.

3. Refresh the MetroCluster configuration using the following steps.

   Do not use the procedures in the section "Configuring the MetroCluster software in ONTAP" found in the Fabric-attached MetroCluster Installation and Configuration Guide.

   a. Enter advanced privilege mode:
      
      `set -privilege advanced`

   b. Refresh the MetroCluster configuration:
      
      `metrocluster configure -refresh true`

   **Example**

   The following command refreshes the MetroCluster configuration on all the nodes in the DR group that contains controller_A_1:

   ```
   controller_A_1:*> metrocluster configure -refresh true
   [Job 009] Job succeeded: Configure is successful.
   ```
c. Return to admin privilege mode:

```
set -privilege admin
```

4. Check the MetroCluster configuration for errors and verify that it is operational.

You should use the procedures in the following sections of the *Fabric-attached MetroCluster Installation and Configuration Guide*:

- Checking for MetroCluster configuration errors with Config Advisor
- Verifying local HA operation
- Verifying switchover, healing, and switchback
Where to find additional information

You can learn more about MetroCluster configuration and operation from the NetApp documentation library.

**MetroCluster and miscellaneous guides**

<table>
<thead>
<tr>
<th>Guide</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ONTAP 9 Documentation Center</strong></td>
<td>• All MetroCluster guides</td>
</tr>
</tbody>
</table>
  • Best practices for MetroCluster FC configuration.     |
| **Fabric-attached MetroCluster installation and configuration** | • Fabric-attached MetroCluster architecture                             
  • Cabling the configuration                            
  • Configuring the FC-to-SAS bridges                   
  • Configuring the FC switches                        
  • Configuring the MetroCluster in ONTAP               |
| **MetroCluster IP installation and configuration**  | • MetroCluster IP architecture                                         
  • Cabling the configuration                           
  • Configuring the MetroCluster in ONTAP               |
| **MetroCluster management and disaster recovery**   | • Understanding the MetroCluster configuration                           
  • Switchover, healing and switchback                  
  • Disaster recovery                                   |
<table>
<thead>
<tr>
<th>Guide</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MetroCluster Service Guide</strong></td>
<td>• Guidelines for maintenance in a MetroCluster FC configuration</td>
</tr>
<tr>
<td></td>
<td>• Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches</td>
</tr>
<tr>
<td></td>
<td>• Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster FC configuration</td>
</tr>
<tr>
<td></td>
<td>• Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster FC configuration</td>
</tr>
<tr>
<td></td>
<td>• Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster FC configuration</td>
</tr>
<tr>
<td></td>
<td>• Expanding a two-node fabric-attached or stretch MetroCluster FC configuration to a four-node MetroCluster configuration</td>
</tr>
<tr>
<td></td>
<td>• Expanding a four-node fabric-attached or stretch MetroCluster FC configuration to an eight-node MetroCluster FC configuration</td>
</tr>
<tr>
<td><strong>MetroCluster Tiebreaker Software Installation and Configuration Guide</strong></td>
<td>• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software</td>
</tr>
<tr>
<td><strong>Active IQ Unified Manager documentation</strong></td>
<td>• Monitoring the MetroCluster configuration and performance</td>
</tr>
<tr>
<td><strong>NetApp Documentation: Product Guides and Resources</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Copy-based transition</strong></td>
<td>• Transitioning data from 7-Mode storage systems to clustered storage systems</td>
</tr>
<tr>
<td><strong>ONTAP concepts</strong></td>
<td>• How mirrored aggregates work</td>
</tr>
</tbody>
</table>
Copyright

Copyright © 2019 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).
Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

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.

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., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

6500N bridges
   FibreBridge, cabling with disk shelves using IOM6 or IOM3 modules 37

A
   about this guide
      deciding whether to use the Stretch MetroCluster Installation and Configuration Guide 6

   access considerations
      after MetroCluster switchover operations when using unmirrored aggregates 10

   Active IQ Unified Manager
      monitoring with 84

   adapters, FC-VI
      cabling controllers to each other and the storage shelves in MetroCluster configurations 17

   aggregates
      mirrored data, creating on each node of a MetroCluster configuration 60, 61

   architecture
      of two-node bridge-attached stretch MetroCluster configurations 20
      of two-node MetroCluster configurations 14

   array LUNs
      example of stretch MetroCluster configurations with 80

   array LUNs and disks
      overview of stretch MetroCluster configurations with 80

   array LUNs, E-Series
      example of stretch MetroCluster configurations with 82

   automatic switchover
      supported MetroCluster configurations 7

   AutoSupport
      worksheet for gathering network information for site A in MetroCluster configurations 41
      worksheet for gathering network information for site B in MetroCluster configurations 42

B
   bridges
      FibreBridge 6500N, cabling with disk shelves using IOM6 or IOM3 modules 37
      installing FC-to-SAS 26

C
   cables, SAS optical
      cabling in stretch MetroCluster systems with SAS shelves 16

   cabling
      controller FC-VI adapters and SAS ports in MetroCluster configurations 17

      controller FC-VI adapters in MetroCluster configurations 17
      controller SAS ports in MetroCluster configurations 17
      data ports 19, 26
      management ports 19, 26
      stretch MetroCluster components 16

   chassis
      verifying the HA state in a stretch MetroCluster configuration 49

   cluster configuration backup files
      providing additional protection 69

   cluster configurations
      similarities and differences between MetroCluster configurations and 44

   cluster peer relationships
      creating 58
      creating relationships between clusters using passphrases 56
      prerequisites for 8

   cluster peering
      considerations when peering a cluster from the MetroCluster site to a third cluster 85
      introduction to MetroCluster configuration 52
      worksheet for gathering network information for site A in MetroCluster configurations 41
      worksheet for gathering network information for site B in MetroCluster configurations 42

   cluster peering connections
      cabling in MetroCluster configurations 18, 25

   Cluster Setup wizard
      using to set up a cluster in a two-node MetroCluster configuration 50

   clustered MetroCluster configurations
      differences between the types 7

   clusters
      example names in MetroCluster configuration 15
      naming conventions in two-node bridge-attached stretch MetroCluster documentation 21
      setting up in a two-node MetroCluster configuration 50

   commands
      using metrocluster configure to start data protection in MetroCluster configurations 63

   volume 94

   comments
      how to send feedback about documentation 102

   components
      racking 17
      racking in a MetroCluster configuration 24

   components, stretch MetroCluster
      installing and cabling 16

   Config Advisor
      checking for common configuration errors 68
      checking for MetroCluster configuration errors 68

   configurations, cluster
      similarities and differences between MetroCluster configurations and 44

   configurations, MetroCluster
similarities and differences between standard cluster configurations and 44
considerations when removing MetroCluster configurations 83
controller FC-VI adapters cabling both the remote and local storage stacks in MetroCluster configurations 17
cabling controller module ports checking connectivity with the partner site in MetroCluster configurations 18, 25
controller modules cabling FC-to-SAS bridges to, in two-node direct-attached MetroCluster configurations 38
resetting to system defaults when reusing, in MetroCluster configurations 45
controller SAS ports cabling both the remote and local storage stacks in MetroCluster configurations 17
controller, storage cabling management and data connections 19, 26
controllers racking 17 verifying the HA state in a stretch MetroCluster configuration 49
creating custom job automatically on partner clusters, using Configuration Replication Service 85
creation, LIFs in a MetroCluster configuration 86
data aggregates mirrored, creating on each node of a MetroCluster configuration 60, 61
data ports cabling 19, 26
considerations when sharing with intercluster LIFs 9
data protection mirroring root aggregates to provide 60
starting in MetroCluster configurations 63
database files how NVFAIL protects 93
databases how NVFAIL protects 93 accessing after a switchover 95
introduction to using NVFAIL to monitor and protect validity of 93
dedicated ports configuring intercluster LIFs to use 53
considerations when using for intercluster replication 9
destination clusters creating relationships with source clusters using passphrases 56
disaster recovery use of SVMs in MCC disaster recovery 90
disk assignments verifying in a two-node MetroCluster configuration 48
disk shelves racking 17
racking in a MetroCluster configuration 24
using IOM12 modules, cabling a FibreBridge 7600N or 7500N bridge with 33
using IOM6 or IOM3 modules, cabling a FibreBridge 6500N bridge with 37
disk shelves, SAS cabling in MetroCluster systems with SAS optical cables 16
installing 26
documentation how to receive automatic notification of changes to 102
how to send feedback about 102
where to find MetroCluster configuration 98
e-E-Series array LUNs example of stretch MetroCluster configurations with 80
events monitoring data loss 94
example names MetroCluster component 15
ExpressNav utility accessing the FibreBridge 7600N bridge 29
fabric-attached MetroCluster configurations considerations for upgrading from stretch MetroCluster configurations to 96
factory configured clusters hardware setup checklist 11
FC MetroCluster configurations verifying operation after loss of a single FC-to-SAS bridge 73
FC switch fabric supported MetroCluster configurations 7
FC switches example names in MetroCluster configuration 15
naming conventions in two-node bridge-attached stretch MetroCluster documentation 21
racking 17
racking in a MetroCluster configuration 24
FC-to-SAS bridge configurations worksheets 23
FC-to-SAS bridges cabling to controller modules in two-node direct-attached MetroCluster configurations 38
configuring for health monitoring 65
considerations for installing SAS shelves and 29
in-band management 27
installing 26
meeting preinstallation requirements 27
naming conventions in two-node bridge-attached stretch MetroCluster documentation 21
supported MetroCluster configurations 7
FC-VI adapters cabling controllers to each other and the storage shelves in MetroCluster configurations 17
FC-VI ports cabling 25
configuring on a X1132A-R6 quad-port card on FAS8020 systems 46
feedback
  how to send comments about documentation 102
FibreBridge 6500N bridges
cabling for disk shelves with IOM6 or IOM3 modules 37
FibreBridge 7500N bridges
cabling for shelves with IOM6 or IOM3 modules 35
FibreBridge 7600N bridges
cabling for shelves with IOM6 or IOM3 modules 35
  enabling IP port access 29
FibreBridge 7600N or 7500N bridges
cabling with disk shelves using IOM12 modules 33
FibreBridge bridges
cabling to controller modules in two-node direct-attached MetroCluster configurations 38
FlexGroup support
  in a MetroCluster configuration 85
four-node MetroCluster configurations implementing 63
FTP
  accessing the FibreBridge 7600N bridge 29

G
guidelines
  for networking and LIF creation 86
guides
  requirements for using the Stretch MetroCluster Installation and Configuration Guide 6

H
HA states
  verifying and setting in a stretch MetroCluster configuration 49
  ha-config settings
    verifying in a stretch MetroCluster configuration 49
hardware components
  rack 17
  racking in a MetroCluster configuration 24
hardware setup
  checklist for factory configured clusters 11
healing
  verifying in a MetroCluster configuration 68
high availability
  requirements for using the Stretch MetroCluster Installation and Configuration Guide 6
host names
  worksheet for gathering network information for site A in MetroCluster configurations 41
  worksheet for gathering network information for site B in MetroCluster configurations 42

I
ICMP
  accessing the FibreBridge 7600N bridge 29
  how to send feedback about improving documentation 102
installation
  for systems with array LUNs 13
  for systems with native disks 13
  preparations for installing FC-to-SAS bridges 27
intercluster LIFs
  configuring to share data ports 55
  configuring to use dedicated intercluster ports 53
  considerations when sharing with data ports 9
  using to create cluster peer relationships 58
intercluster networks
  configuring intercluster LIFs to share data ports 55
  configuring intercluster LIFs to use dedicated intercluster ports 53
  considerations when sharing data and intercluster ports 9
intercluster ports
  considerations when using dedicated 9
IOM12 modules
  cabling a FibreBridge 7600N or 7500N bridge with disk shelves using 33
IOM3 modules
  cabling a FibreBridge 6500N bridge with disk shelves using 37
IOM6 modules
  cabling a FibreBridge 6500N bridge with disk shelves using 37
IP addresses
  worksheet for gathering network information for site A in MetroCluster configurations 41
  worksheet for gathering network information for site B in MetroCluster configurations 42
IP switch fabric
  supported MetroCluster configurations 7
IPSpace objects
  replication requirements 86
issues
  LIF replication and placement 87

L
LDAP client configuration
  in a MetroCluster configuration 85
licenses
  considerations when using ONTAP in MetroCluster configurations 85
LIF creation
  in a MetroCluster configuration 86
  requirements 87
LIF placement
  requirements 87
LIF replication
  in a MetroCluster configuration 86
  requirements 87
local HA
  supported MetroCluster configurations 7
LUNs
  recovering after NVRAM failures 95

M
management ports
  cabling 19, 26
MetroCluster
SVM resynchronization following disaster 91
MetroCluster components
racking disk shelves 17, 24
racking FC switches 17, 24
racking storage controllers 17, 24
MetroCluster configuration
bridge-attached stretch, workflow for cabling two
nodes 20
checking for configuration errors with Config
Advisor 68
LDAP client configuration 85
SAS-attached stretch, workflow for cabling two
nodes 14
workflow for 26
MetroCluster configurations
access considerations after switchover operations
when using unmirrored aggregates 10
architecture of direct-attached two-node 14
cabling cluster peering connections 18, 25
cabling controllers to each other and the storage
shelves 17
cabling FC-VI adapters 25
cabling HBA adapters 25
cabling MetroCluster components 25
configuring FC-to-SAS bridges for health
monitoring 65
considerations when removing 83
creating mirrored data aggregates on each node of
60, 61
direct-attached MetroCluster configurations
parts of 14
preconfigured settings for new MetroCluster systems
from the factory 10
similarities and differences between standard cluster
configurations and 44
SnapMirror support and licensing considerations
when using ONTAP in 85
verifying correct operation of 66
verifying manual switchback after negotiated
switchover 71
verifying negotiated switchover 70
verifying operation after loss of a single storage shelf
75
verifying operation after power line disruption 74
where to find information about 98
MetroCluster configurations, stretch
example configurations with array LUNs and disks
80
MetroCluster configurations, stretch with E-Series array
LUNs
example 82
metrocluster configure command
creating MetroCluster relationships using 63
MetroCluster monitoring
using Tiebreaker software 68
MetroCluster switchovers
output for the storage aggregate plex show command
is indeterminate after 92
MetroCluster systems, stretch
installing and cabling components 16
N
naming conventions
in two-node bridge-attached stretch MetroCluster
documentation 21
network information
worksheet for gathering for site A in MetroCluster
configurations 41
worksheet for gathering for site B in MetroCluster
configurations 42
NFS LUNs
how NVFAIL impacts access to 93
NFS volumes
how NVFAIL impacts access to 93
node configuration after MetroCluster setup
additional configuration with ONTAP System
Manager 84
nodes
creating mirrored data aggregates on each
MetroCluster 60, 61
similarities and differences between standard cluster
and MetroCluster configurations 44
using the Cluster Setup wizard to set up, in a two-
node MetroCluster configuration 50
NTP servers
configuring to synchronize system time 84
NVFAIL
description of 93
how it impacts access to NFS volumes or LUNs 93
modifying volumes to set NVFAIL in case of
switchover 93
NVRAM failures
recovering LUNs after 95
O
ONTAP health monitoring
configuring FC-to-SAS bridges for 65
ONTAP System Manager
node configuration with 84
optical cables, SAS
cabling in stretch MetroCluster systems with SAS
shelves 16
P
partner clusters
cabling cluster peering connections in MetroCluster
configurations 18, 25
peering clusters
MetroCluster configuration, introduction to 52
ports
considerations when using dedicated intercluster 9
ports, data
cabling 19, 26
ports, management
cabling 19, 26
ports, SAS
cabling controllers to each other and the storage
shelves in MetroCluster configurations 17
preconfigured settings
for new MetroCluster systems from the factory 10
Q

QuickNAV utility
accessing the FibreBridge 7600N bridge 29

R

relationships
creating for MetroCluster 63
remote URLs
using to provide additional protection 69
removing
MetroCluster configurations, considerations 83
replication
of job schedule for a MetroCluster configuration, user-created 85
replication, IPSpace objects
requirements 86
replication, LIFs
in a MetroCluster configuration 86
required hardware
MetroCluster 15
required hardware components
for two-node bridge-attached stretch MetroCluster configurations 21
requirements
for LIF creation when configuring network 87
for LIF replication and placement 87
IPSpace object replication 86
subnet configuration 86
worksheet for gathering network information for site A in MetroCluster configurations 41
worksheet for gathering network information for site B in MetroCluster configurations 42
requirements for cluster peering relationships
listed 8
root aggregates
mirroring 60
volume creation on 90

S

SAS disk shelves
installing 26
SAS optical cables
cabling in stretch MetroCluster systems with SAS shelves 16
SAS optical configuration
documented in the Stretch MetroCluster Installation and Configuration Guide 6
SAS ports
cabling controllers to each other and the storage shelves in MetroCluster configurations 17
SAS shelves
cabling in MetroCluster systems with SAS optical cables 16
considerations for installing FC-to-SAS bridges and 29
SAS storage, bridge-attached
supported MetroCluster configurations 7
SAS storage, direct-attached
supported MetroCluster configurations 7
Service Processors
worksheet for gathering network information for site A in MetroCluster configurations 41
worksheet for gathering network information for site B in MetroCluster configurations 42
shared ports
configuring intercluster LIFs for intercluster networking 55
shelves
using IOM6 or IOM3 modules, cabling a FibreBridge 7600N or 7500N bridge with 35
shelves, SAS
cabling in MetroCluster systems with SAS optical cables 16
installing 26
site configurations
worksheet for gathering network information for site A in MetroCluster configurations 41
worksheet for gathering network information for site B in MetroCluster configurations 42
SnapMirror support
consideration when using ONTAP in MetroCluster configurations 85
SNMP
accessing the FibreBridge 7600N bridge 29
software configuration
workflow for MetroCluster in ONTAP 40
source clusters
creating relationships with destination clusters using passphrases 56
storage aggregate plex show command
output is indeterminate after a MetroCluster switchover 92
storage controller
cabling management and data connections 19, 26
storage controllers
example names in MetroCluster configuration 15
naming conventions in two-node bridge-attached stretch MetroCluster documentation 21
racking in a MetroCluster configuration 24
storage disk show command
output in a two-node stretch MetroCluster configuration 92
storage shelf show command
output in a two-node stretch MetroCluster configuration 92
stretch MetroCluster configuration with E-Series array LUNs
element 82
stretch MetroCluster configurations
considerations for upgrading to fabric-attached MetroCluster configurations 96
example configurations with array LUNs and disks 80
verifying chassis and controller HA state 49
with array LUNs, connectivity 80
stretch MetroCluster configurations with array LUNs
element 80
Stretch MetroCluster Installation and Configuration Guide
requirements for using 6
stretch MetroCluster systems
installing and cabling components 16
subnet configuration
requirements 86
suggestions
how to send feedback about documentation 102
SVMs
as sources for MCC disaster recovery 90
resynchronization following disaster 91
switchback
verifying in a MetroCluster configuration 68
switchover
accessing the database after 95
verifying in a MetroCluster configuration 68
system defaults
resetting reused controller modules to, in
MetroCluster configurations 45
system time
synchronizing using NTP 84
systems, stretch MetroCluster
installing and cabling components 16

T
telnet
accessing the FibreBridge 7600N bridge 29
Tiebreaker software
installing 68
using to identify failures 68
tools
checking for MetroCluster configuration errors with
Config Advisor 68
downloading and running Config Advisor 68
Twitter
how to receive automatic notification of
documentation changes 102
two-node bridge-attached stretch MetroCluster
configurations
illustration of 20
naming conventions 21
parts of 20
required hardware components 21
two-node direct-attached MetroCluster configurations
cabling FC-to-SAS bridges to controller modules in
38
two-node MetroCluster configurations
implementing 63
setting up clusters in 50
verifying disk assignments 48
unmirrored aggregates
access considerations after MetroCluster switchover
operations 10
upgrades
from stretch to fabric-attached MetroCluster
configurations 96
user-created job schedules
replicated automatically in MetroCluster
configurations 85
utilities
checking for MetroCluster configuration errors with
Config Advisor 68
downloading and running Config Advisor 68

V
verifying
chassis components and controller HA state in a
MetroCluster configuration 49
volume creation
in a MetroCluster configuration 90
volumes
commands 94
recovering after a switchover 95
workflows
cabling a two-node bridge-attached stretch
MetroCluster configuration 20
cabling a two-node SAS-attached stretch
MetroCluster configuration 14
MetroCluster software configuration in ONTAP 40
worksheets
for FC-to-SAS bridge configurations 23
for gathering network information for site A in
MetroCluster configurations 41
for gathering network information for site B in
MetroCluster configurations 42

X
X1132A-R6 quad-port cards
configuring FC-VI ports on FAS8020 systems 46