MetroCluster Documentation

ONTAP MetroCluster

NetApp
September 24, 2021

Table of Contents

MetroCluster Documentation

MetroCluster

The ONTAP 9 Release Notes describe new features, upgrade notes, fixed issues, known limitations, and known issues.

You are required to sign on to the NetApp Support Site to access the Release Notes.

Fabric-attached MetroCluster Installation and Configuration Guide

This guide describes how to install and configure the MetroCluster hardware and software components in a fabric configuration.

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

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

Preparing for the MetroCluster installation

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

Differences among the ONTAP MetroCluster configurations

Differences between ONTAP MetroCluster configurations

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

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

Feature	IP configurations	Fabric attached configurations		Stretch configurations	
		Four- or eight-node	Two-node	Two-node bridge-attached	Two-node direct-attached
Number of controllers	Four or eight*	Four or eight	Two	Two	Two
Uses an FC switch storage fabric	No	Yes	Yes	No	No
Uses an IP switch storage fabric	Yes	No	No	No	No
Uses FC-to-SAS bridges	No	Yes	Yes	Yes	No

Uses direct-attached SAS storage	Yes (local attached only)	No	No	No	Yes
Supports ADP	Yes (starting in ONTAP 9.4)	No	No	No	No
Supports local HA	Yes	Yes	No	No	No
Supports ONTAP AUSO	No	Yes	Yes	Yes	Yes
Supports unmirrored aggregates	Yes (starting in ONTAP 9.8)	Yes	Yes	Yes	Yes
Supports array LUNs	No	Yes	Yes	Yes	Yes
Supports ONTAP Mediator	Yes (starting in ONTAP 9.7)	No	No	No	No
Supports MetroCluster Tiebreaker	Yes (not in combination with ONTAP Mediator)	Yes	Yes	Yes	Yes
Supports All SAN Arrays	Yes	Yes	Yes	Yes	Yes

Important

Notice the following considerations for eight-node MetroCluster IP configurations:

- Eight-node configurations are supported starting in ONTAP 9.9.1.
- Only NetApp-validated MetroCluster switches (ordered from NetApp) are supported.
- Configurations using IP-routed (layer 3) backend connections are not supported.
- Configurations using shared private layer 2 networks are not supported.
- Configurations using a Cisco 9336C-FX2 shared switch are not supported.

Support for All SAN Array systems in MetroCluster configurations

Some of the All SAN Arrays (ASAs) are supported in MetroCluster configurations. In the MetroCluster documentation, the information for AFF models applies to the corresponding ASA system. For example, all cabling and other information for the AFF A400 system also applies to the ASA AFF A400 system.

Supported platform configurations are listed in the NetApp Hardware Universe.

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.

Each MetroCluster site is configured as a peer to its partner site. You must be familiar with the prerequisites and guidelines for configuring the peering relationships. This is important when deciding on 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 connectivity between 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 used in each cluster must meet the following requirements:

- The subnet must have enough IP addresses available to allocate to one intercluster LIF per node.

  For example, in a six-node cluster, the subnet used for intercluster communication must have six available IP addresses.

Each node must have an intercluster LIF with an IP address on the intercluster network.

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

> ONTAP 9 enables you to migrate your peering networks from IPv4 to IPv6 by optionally allowing both protocols to be present simultaneously on the intercluster LIFs. In earlier releases, all intercluster relationships for an entire cluster were either IPv4 or IPv6. This meant that changing protocols was a potentially disruptive event.

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 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 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
- Bidirectional HTTPS between the intercluster LIFs

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 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. This 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 the 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. This 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 for MetroCluster configurations with native disk shelves or array LUNs

The MetroCluster configuration supports installations with native (NetApp) disk shelves only, array LUNs only, or a combination of both.

AFF systems do not support array LUNs.

Related information

Cabling a fabric-attached MetroCluster configuration

Planning and installing a MetroCluster configuration with array LUNs

FlexArray virtualization installation requirements and reference

Considerations when transitioning from 7-Mode to ONTAP

You must have the new MetroCluster configuration fully configured and operating before you use the transition tools to move data from a 7-Mode MetroCluster configuration to an ONTAP configuration. If the 7-Mode configuration uses Brocade 6510 switches, the new configuration can share the existing fabrics to reduce the hardware requirements.

If you have Brocade 6510 switches and plan on sharing the switch fabrics between the 7-Mode fabric MetroCluster and the MetroCluster running in ONTAP, you must use the specific procedure for configuring the MetroCluster components.

Configuring the MetroCluster hardware for sharing a 7-Mode Brocade 6510 FC fabric during transition

Considerations for ISLs

You must determine how many ISLs you need for each FC switch fabric in the MetroCluster configuration. Beginning with ONTAP 9.2, in some cases, instead of dedicating FC switches and ISLs to each individual MetroCluster configuration, you can share the same four switches.

ISL sharing considerations (ONTAP 9.2)

Starting with ONTAP 9.2, you can use ISL sharing in the following cases:

- One two-node and one four-node MetroCluster configurations
- Two separate four-node MetroCluster configurations
- Two separate two-node MetroCluster configurations
- Two DR groups within one eight-node MetroCluster configuration

The number of ISLs required between the shared switches depends on the bandwidth of the platform models connected to the shared switches.

Consider the following aspects of your configuration when determining how many ISLs you need.

- Non-MetroCluster devices should not be connected to any of the FC switches that provide the back-end MetroCluster connectivity.
- ISL sharing is supported on all switches except the Cisco 9250i and Cisco 9148 switches.
- All nodes must be running ONTAP 9.2 or later.
- The FC switch cabling for ISL sharing is the same as for the eight-node MetroCluster cabling.
- The RCF files for ISL sharing are same as for the eight-node MetroCluster cabling.
- You should verify that all hardware and software versions are supported.

  NetApp Hardware Universe

- The speed and number of ISLs must be sized to support the client load on both MetroCluster systems.
- The back-end ISLs and the back-end components must be dedicated to the MetroCluster configuration only.
- The ISL must use one of the supported speeds: 4 Gbps, 8 Gbps, 16 Gbps, or 32 Gbps.
- The ISLs on one fabric should all be the same speed and length.
- The ISLs on one fabric should all have the same topology. For example, they should all be direct links, or if your system uses WDM, then they should all use WDM.

Platform-specific ISL considerations

The number of recommended ISLs is platform-model specific. The following table shows the ISL requirements for each fabric by platform model. It assumes that each ISL has a 16-Gbps capacity.

Platform model	Recommended number of ISLs per four-node DR group (per switch fabric)
AFF A700	Six
FAS9000	Six
8080	Four
All others	Two

If the switch fabric is supporting eight nodes (either part of a single, eight-node MetroCluster configuration, or two four-node configurations that are sharing ISLs), the recommended total number of ISLs for the fabric is the sum of that required for each four-node DR group. For example:

- If DR group 1 includes four AFF A700 systems, it requires six ISLs.
- If DR group 2 includes four FAS8200 systems, it requires two ISLs.
- The total number of recommended ISLs for the switch fabric is eight.

Considerations for using TDM/WDM equipment with fabric-attached MetroCluster configurations

The Hardware Universe tool provides some notes about the requirements that Time Division Multiplexing (TDM) or Wavelength Division Multiplexing (WDM) equipment must meet to work with a fabric-attached MetroCluster configuration. These notes also include information about various configurations, which can help you to determine when to use in-order delivery (IOD) of frames or out-of-order delivery (OOD) of frames.

An example of such requirements is that the TDM/WDM equipment must support the link aggregation (trunking) feature with routing policies. The order of delivery (IOD or OOD) of frames is maintained within a switch, and is determined by the routing policy that is in effect.

NetApp Hardware Universe

The following table provides the routing policies for configurations containing Brocade switches and Cisco switches:

Switches	Configuring MetroCluster configurations for IOD	Configuring MetroCluster configurations for OOD
Brocade	• AptPolicy must be set to 1 • DLS must be set to off • IOD must be set to on	• AptPolicy must be set to 3 • DLS must be set to on • IOD must be set to off
Cisco	Policies for the FCVI-designated VSAN: • Load balancing policy: srcid and dstid • IOD must be set to on Policies for the storage-designated VSAN: • Load balancing policy: srcid, dstid, and oxid • VSAN must not have the in-order-guarantee option set	Not applicable

When to use IOD

It is best to use IOD if it is supported by the links. The following configurations support IOD:

- A single ISL
- The ISL and the link (and the link equipment, such as TDM/WDM, if used) supports configuration for IOD.
- A single trunk, and the ISLs and the links (and the link equipment, such as TDM/WDM, if used) support configuration for IOD.

When to use OOD

- You can use OOD for all configurations that do not support IOD.
- You can use OOD for configurations that do not support the trunking feature.

Using encryption devices

When using dedicated encryption devices on the ISL or encryption on WDM devices in the MetroCluster configuration, you must meet the following requirements:

- The external encryption devices or WDM equipment has been self certified by the vendor with the FC switch in question.

  The self certification should cover the operating mode (such as trunking and encryption).

- The added latency due to encryption should be no more than 10 microseconds.

Requirements for using a Brocade DCX 8510-8 switch

- The DCX 8510-8 switches used in MetroCluster configurations must be purchased from NetApp.
- For scalability, you should leave one port-chunk between MetroCluster configurations if cabling only two MetroClusters in 4x48-port modules. This enables you to expand port usage in MetroCluster configurations without recabling.
- Each Brocade DCX 8510-8 switch in the MetroCluster configuration must be correctly configured for the ISL ports and storage connections. For port usage, see the following section: Port assignments for FC switches when using ONTAP 9.1 and later.
- ISLs cannot be shared and each MetroCluster requires two ISLs for each fabric.
- The DCX 8510-8 switch used for backend MetroCluster connectivity should not be used for any other connectivity.

  Non-MetroCluster devices should not be connected to these switches and non-MetroCluster traffic should not flow through DCX 8510-8 switches.

- One line card can either be connected to ONTAP MetroClusters **or** ONTAP 7-Mode MetroClusters.

RCF files are not available for this switch.

The following are the requirements for using two Brocade DCX 8510-8 switches:

- You must have one DCX 8510-8 switch at each site.
- You must use a minimum of two 48-port blades that contain 16Gb SFPs in each switch.

The following are the requirements for using four DCX 8510-8 switches at each site in a MetroCluster configuration:

- You must have two DCX 8510-8 switches at each site.
- You must use at least one 48-port blade for each DCX 8510-8 switch.
- Each blade is configured as a virtual switch using virtual fabrics.

The following NetApp products are not supported by Brocade DCX 8510-8 switches:

- Config Advisor
- Fabric Health Monitor
- MyAutoSupport (system risks might show false positives)
- Active IQ Unified Manager (formerly OnCommand Unified Manager)

> Ensure that all the components needed for this configuration are in the NetApp Interoperability Matrix Tool. Read the notes section in the Interoperability Matrix Tool for information on supported configurations.

Considerations when using unmirrored aggregates

Considerations when using unmirrored aggregates

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

Considerations for unmirrored aggregates when doing maintenance requiring power shutdown

If you are performing a 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 take any unmirrored aggregates offline, 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. This is the result of a power shutdown or a loss of ISLs.

Considerations for unmirrored aggregates and hierarchical namespaces

If you are 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 metadata volume and data SVM root volumes

The configuration replication service (CRS) metadata volume and data SVM root volumes must be on a mirrored aggregate. You cannot move these volumes to an unmirrored aggregate. If they are on an 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

SVMs 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.

Considerations for unmirrored aggregates and SAN

In ONTAP versions prior to 9.9.1, a LUN should not be located on an unmirrored aggregate. Configuring a LUN on an unmirrored aggregate can result in a switchover operation that exceeds 120 seconds and a data outage.

Firewall usage at MetroCluster sites

Considerations for firewall usage at MetroCluster sites

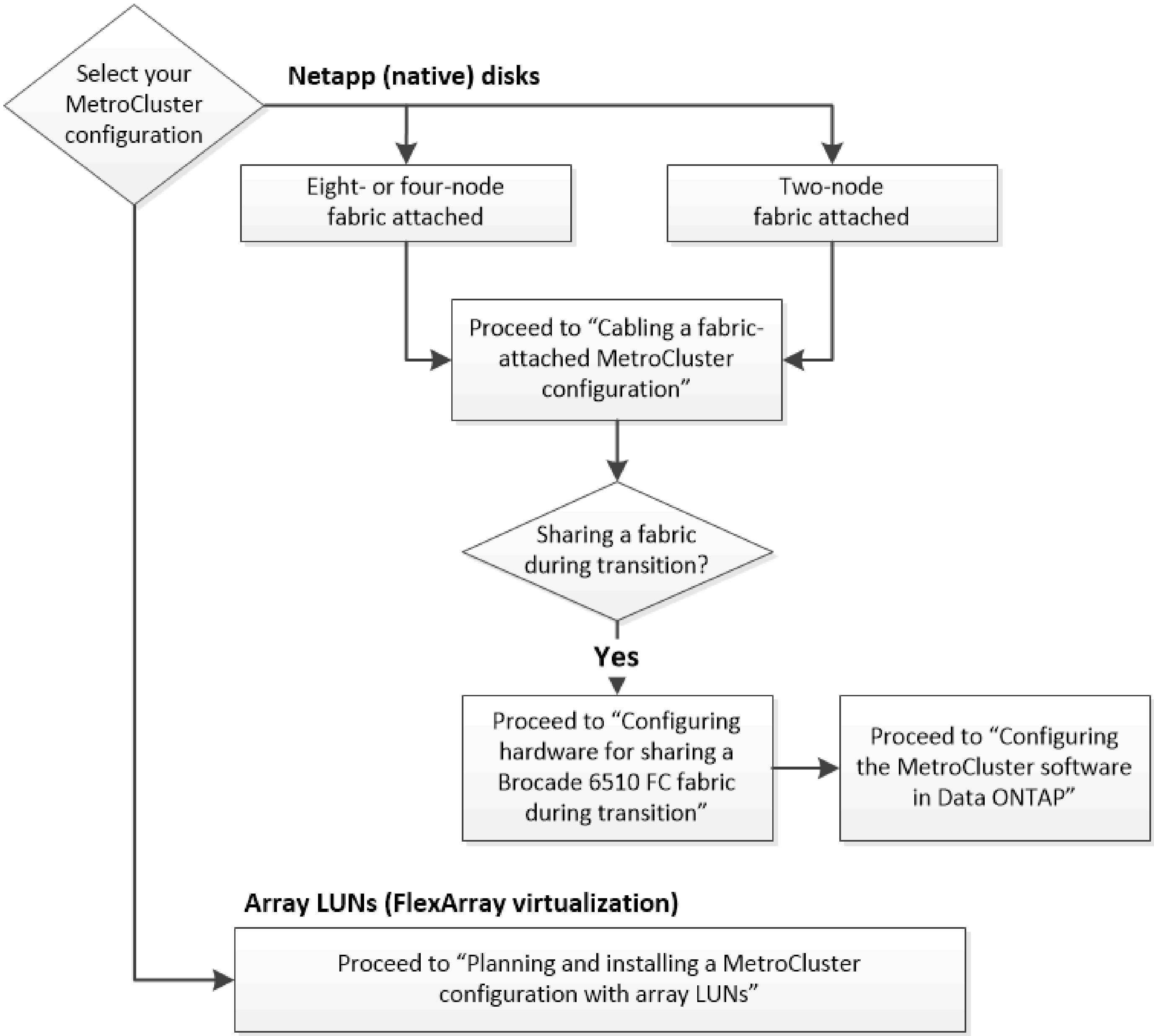
If you are using a firewall at a MetroCluster site, you must ensure access for required ports.

The following table shows TCP/UDP port usage in an external firewall positioned between two MetroCluster sites.

Traffic type	Port/services
Cluster peering	11104 / TCP 11105 / TCP
ONTAP System Manager	443 / TCP
MetroCluster IP intercluster LIFs	65200 / TCP 10006 / TCP and UDP
Hardware assist	4444 / TCP

Choosing the correct installation procedure for your configuration

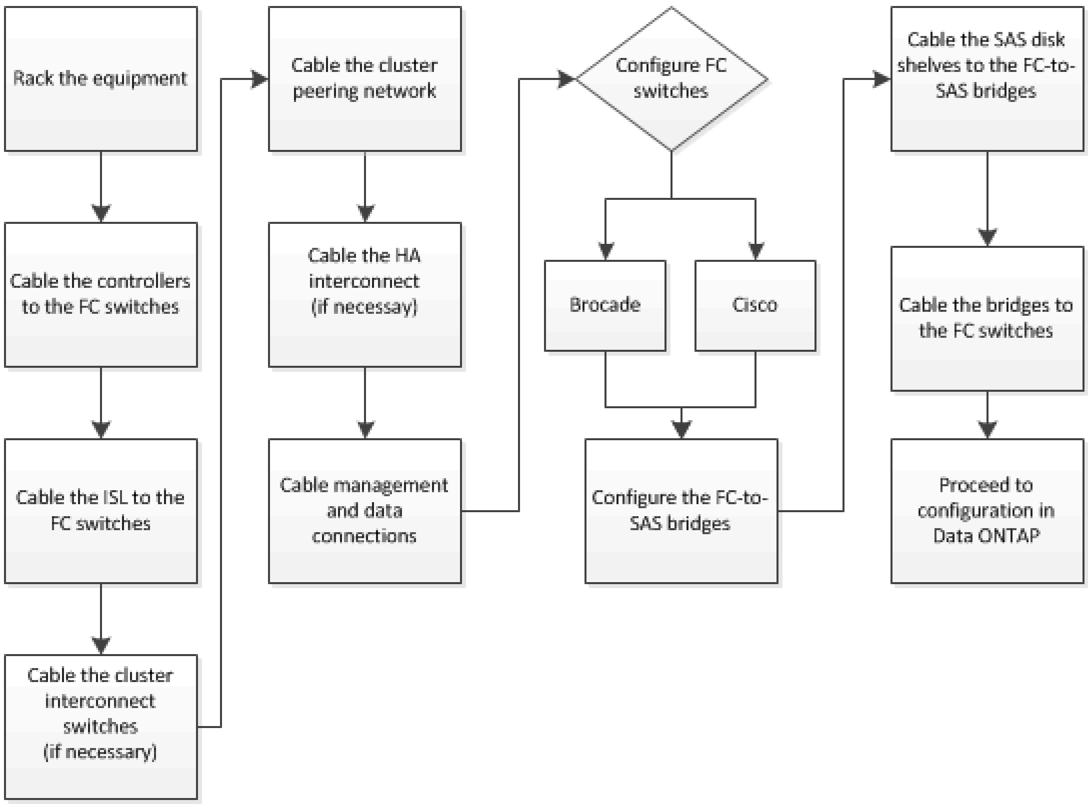
You must choose the correct installation procedure based on whether you are using FlexArray LUNs, the number of nodes in the MetroCluster configuration, and whether you are sharing an existing FC switch fabric used by a 7-Mode fabric MetroCluster.



For this installation type…	Use these procedures…
Fabric-attached configuration with NetApp (native) disks	1. Cabling a fabric-attached MetroCluster configuration 2. Configuring the MetroCluster software in ONTAP
Fabric-attached configuration when sharing with an existing FC switch fabric This is supported only as a temporary configuration with a 7-Mode fabric MetroCluster configuration using Brocade 6510 switches.	1. Cabling a fabric-attached MetroCluster configuration 2. Configuring the MetroCluster hardware for sharing a 7-Mode Brocade 6510 FC fabric during transition 3. Configuring the MetroCluster software in ONTAP

Cabling a fabric-attached 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.



Parts of a fabric MetroCluster configuration

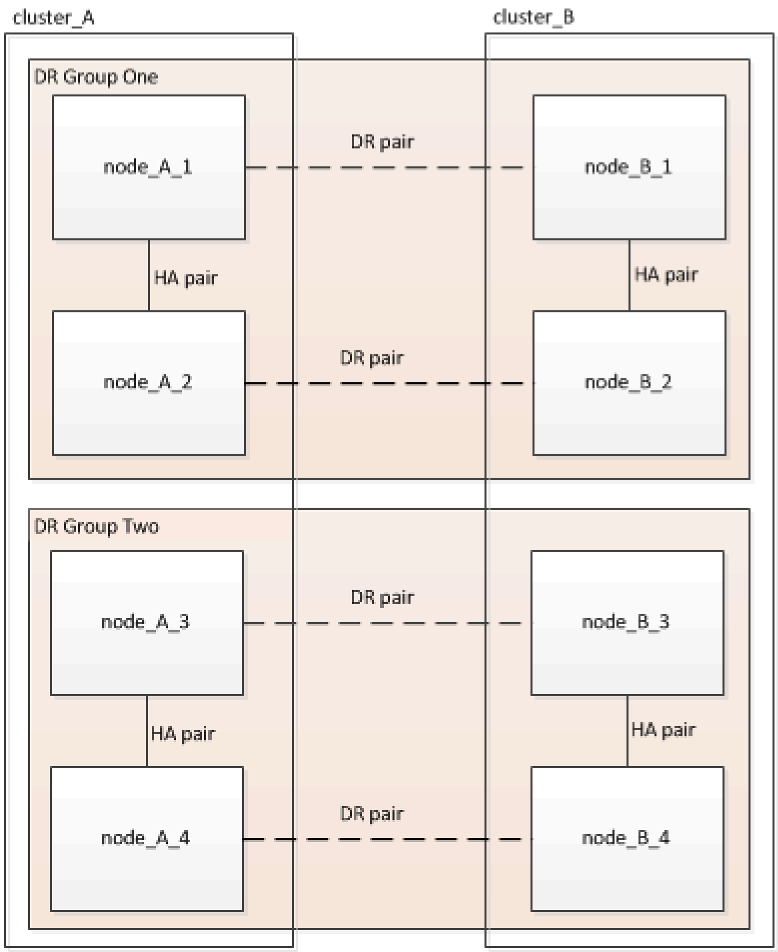
As you plan your MetroCluster configuration, you should understand the hardware components and how they interconnect.

Disaster Recovery (DR) groups

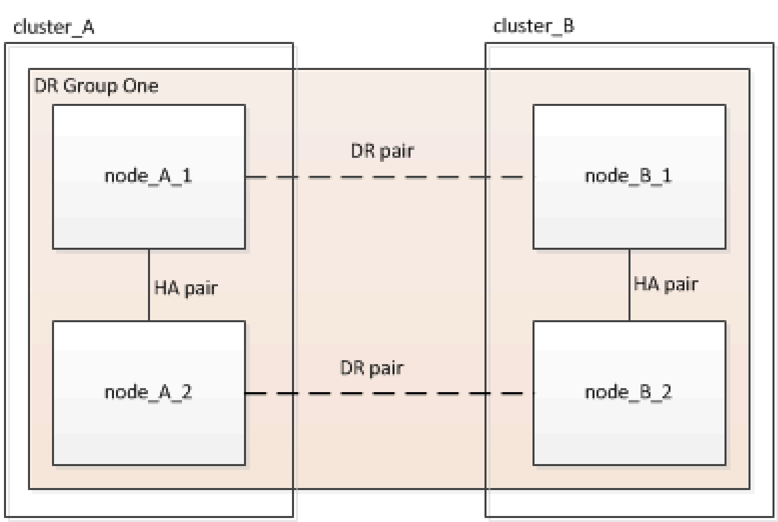
A fabric MetroCluster configuration consists of one or two DR groups, depending on the number of nodes in the MetroCluster configuration. Each DR group consists of four nodes.

- An eight-node MetroCluster configuration consists of two DR groups.
- A four-node MetroCluster configuration consists of one DR group.

The following illustration shows the organization of nodes in an eight-node MetroCluster configuration:



The following illustration shows the organization of nodes in a four-node MetroCluster configuration:



Key hardware elements

A MetroCluster configuration includes the following key hardware elements:

- Storage controllers

  The storage controllers are not connected directly to the storage but connect to two redundant FC switch fabrics.

- FC-to-SAS bridges

  The FC-to-SAS bridges connect the SAS storage stacks to the FC switches, providing bridging between the two protocols.

- FC switches

  The FC switches provide the long-haul backbone ISL between the two sites. The FC switches provide the two storage fabrics that allow data mirroring to the remote storage pools.

- Cluster peering network

  The cluster peering network provides connectivity for mirroring of the cluster configuration, which includes storage virtual machine (SVM) configuration. The configuration of all of the SVMs on one cluster is mirrored to the partner cluster.

Eight-node fabric MetroCluster configuration

An eight-node configuration consists of two clusters, one at each geographically separated site. cluster_A is located at the first MetroCluster site. cluster_B is located at the second MetroCluster site. Each site has one SAS storage stack. Additional storage stacks are supported, but only one is shown at each site. The HA pairs are configured as switchless clusters, without cluster interconnect switches. A switched configuration is supported, but is not shown.

An eight-node configuration includes the following connections:

- FC connections from each controller's HBAs and FC-VI adapters to each of the FC switches
- An FC connection from each FC-to-SAS bridge to an FC switch
- SAS connections between each SAS shelf and from the top and bottom of each stack to an FC-to-SAS bridge
- An HA interconnect between each controller in the local HA pair

  If the controllers support a single-chassis HA pair, the HA interconnect is internal, occurring through the backplane, meaning that an external interconnect is not required.

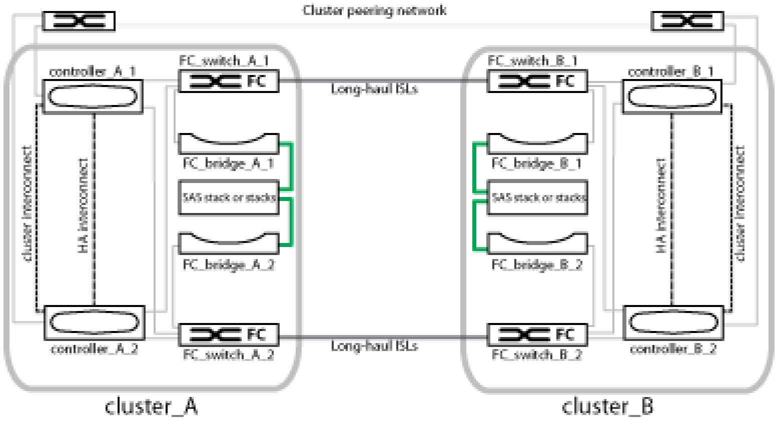
- Ethernet connections from the controllers to the customer-provided network that is used for cluster peering

  SVM configuration is replicated over the cluster peering network.

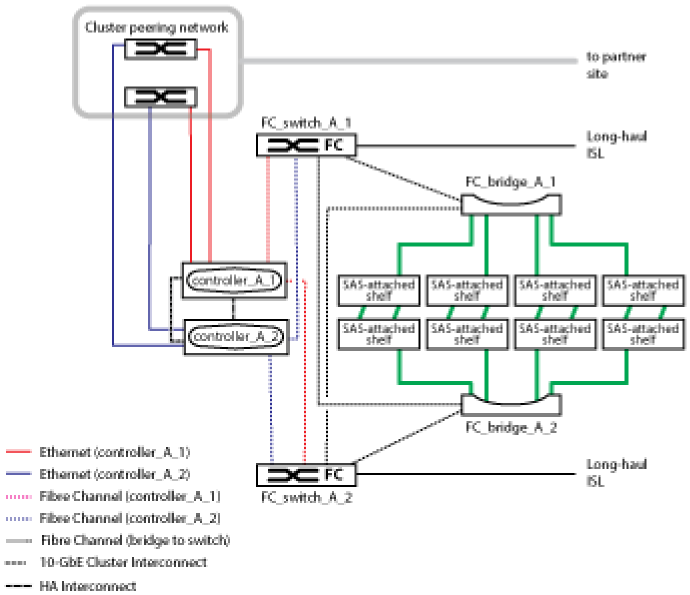
- A cluster interconnect between each controller in the local cluster

Four-node fabric MetroCluster configuration

The following illustration shows a simplified view of a four-node fabric MetroCluster configuration. For some connections, a single line represents multiple, redundant connections between the components. Data and management network connections are not shown.

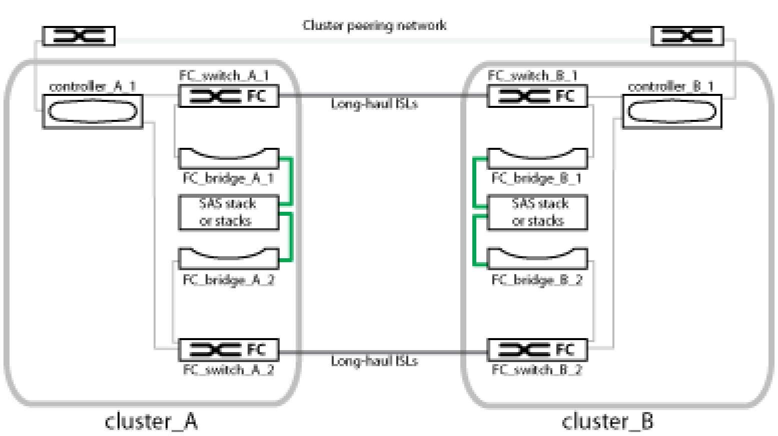


The following illustration shows a more detailed view of the connectivity in a single MetroCluster cluster (both clusters have the same configuration):



Two-node fabric MetroCluster configuration

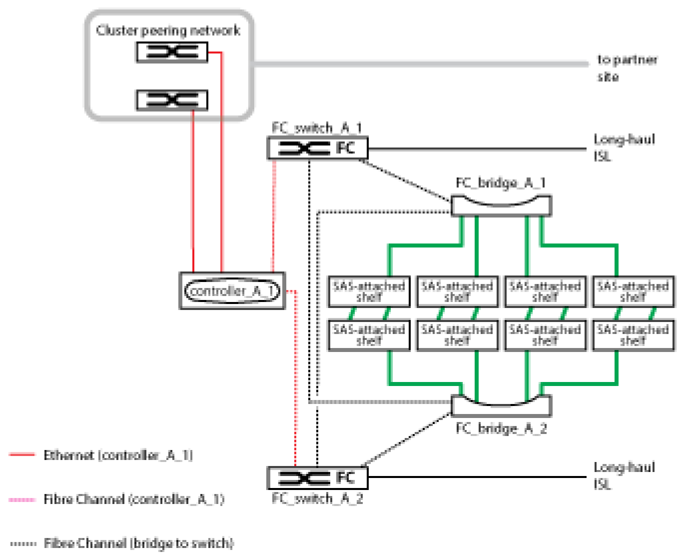
The following illustration shows a simplified view of a two-node fabric MetroCluster configuration. For some connections, a single line represents multiple, redundant connections between the components. Data and management network connections are not shown.



A two-node configuration consists of two clusters, one at each geographically separated site. cluster_A is located at the first MetroCluster site. cluster_B is located at the second MetroCluster site. Each site has one SAS storage stack. Additional storage stacks are supported, but only one is shown at each site.

> In a two-node configuration, the nodes are not configured as an HA pair.

The following illustration shows a more detailed view of the connectivity in a single MetroCluster cluster (both clusters have the same configuration):



A two-node configuration includes the following connections:

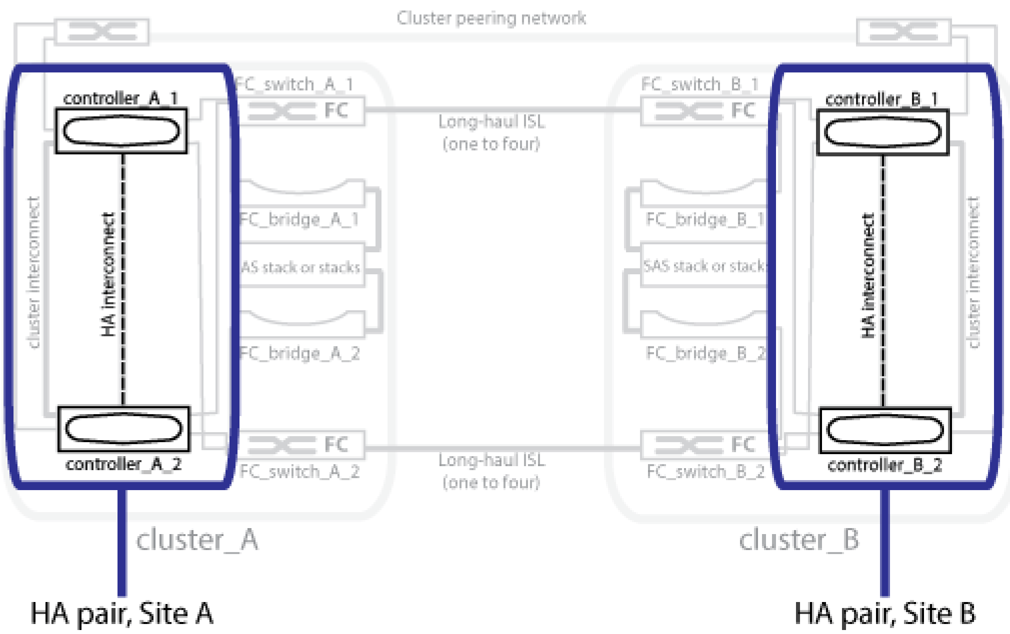
- FC connections between the FC-VI adapter on each controller module
- FC connections from each controller module’s HBAs to the FC-to-SAS bridge for each SAS shelf stack
- SAS connections between each SAS shelf and from the top and bottom of each stack to an FC-to-SAS bridge
- Ethernet connections from the controllers to the customer-provided network that is used for cluster peering

  SVM configuration is replicated over the cluster peering network.

Illustration of the local HA pairs in a MetroCluster configuration

In eight-node or four-node MetroCluster configurations, each site consists of storage controllers configured as one or two HA pairs. This allows local redundancy so that if one storage controller fails, its local HA partner can take over. Such failures can be handled without a MetroCluster switchover operation.

Local HA failover and giveback operations are performed with the storage failover commands, in the same manner as a non-MetroCluster configuration.



Related information

Illustration of redundant FC-to-SAS bridges

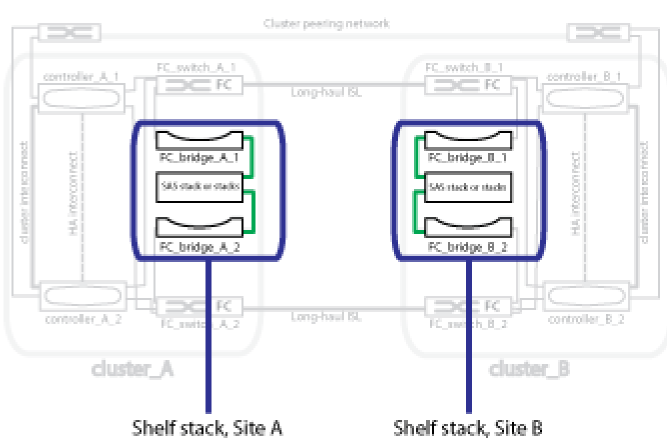
Redundant FC switch fabrics

Illustration of the cluster peering network

ONTAP concepts

Illustration of redundant FC-to-SAS bridges

FC-to-SAS bridges provide protocol bridging between SAS attached disks and the FC switch fabric.



Related information

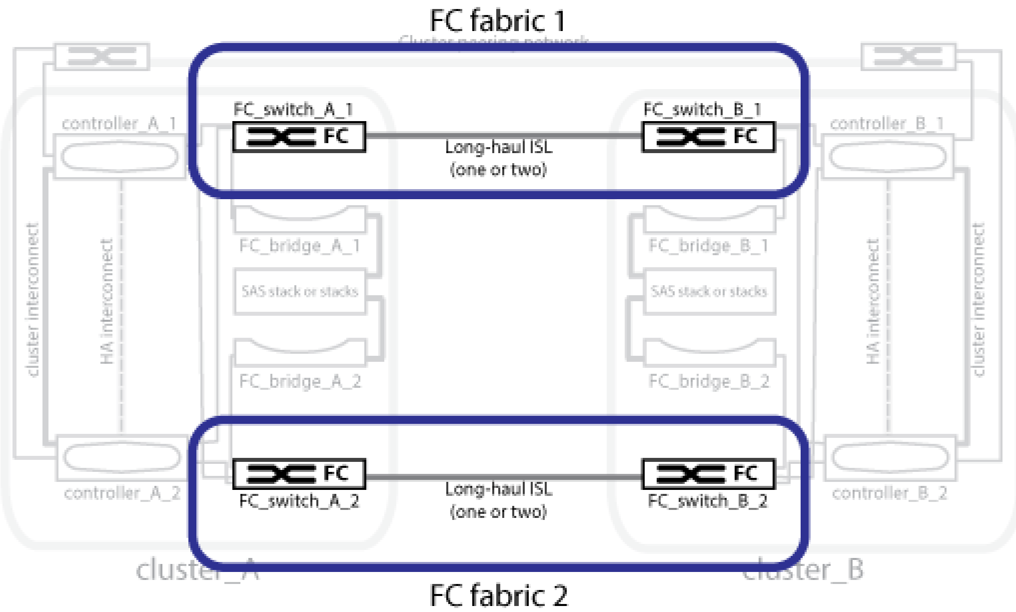
Illustration of the local HA pairs in a MetroCluster configuration

Redundant FC switch fabrics

Illustration of the cluster peering network

Redundant FC switch fabrics

Each switch fabric includes inter-switch links (ISLs) that connect the sites. Data is replicated from site-to-site over the ISL. Each switch fabric must be on different physical paths for redundancy.



Related information

Illustration of the local HA pairs in a MetroCluster configuration

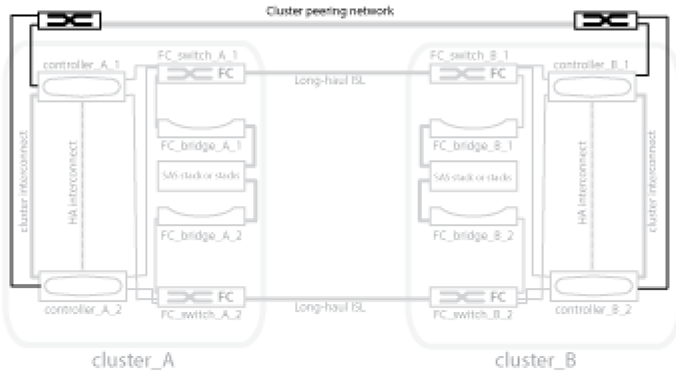
Illustration of redundant FC-to-SAS bridges

Illustration of the cluster peering network

Illustration of the cluster peering network

The two clusters in the MetroCluster configuration are peered through a customer-provided cluster peering network. Cluster peering supports the synchronous mirroring of storage virtual machines (SVMs, formerly known as Vservers) between the sites.

Intercluster LIFs must be configured on each node in the MetroCluster configuration, and the clusters must be configured for peering. The ports with the intercluster LIFs are connected to the customer-provided cluster peering network. Replication of the SVM configuration is carried out over this network through the Configuration Replication Service.



Related information

Illustration of the local HA pairs in a MetroCluster configuration

Illustration of redundant FC-to-SAS bridges

Redundant FC switch fabrics

Cluster and SVM peering express configuration

Considerations for configuring cluster peering

Cabling the cluster peering connections

Peering the clusters

Required MetroCluster FC components and naming conventions

When planning your MetroCluster FC 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.

> Long-wave SFPs are not supported in the MetroCluster storage switches. For a table of supported SPFs, see the MetroCluster Technical Report.

Hardware redundancy in the MetroCluster FC configuration

Because of the hardware redundancy in the MetroCluster FC 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 ONTAP clusters

The fabric-attached MetroCluster FC configuration requires two ONTAP clusters, one at each MetroCluster site.

Naming must be unique within the MetroCluster configuration.

Example names:

- Site A: cluster_A
- Site B: cluster_B

Requirement for four FC switches

The fabric-attached MetroCluster FC configuration requires four FC switches (supported Brocade or Cisco models).

The four switches form two switch storage fabrics that provide the ISL between each of the clusters in the MetroCluster FC configuration.

Naming must be unique within the MetroCluster configuration.

Requirement for two, four, or eight controller modules

The fabric-attached MetroCluster FC configuration requires two, four, or eight controller modules.

In a four or eight-node MetroCluster configuration, the controller modules at each site form one or two HA pairs. Each controller module has a DR partner at the other site.

The controller modules 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.

  However, in configurations with two DR groups, each DR group can consist of different controller module models.

- 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 four cluster interconnect switches

The fabric-attached MetroCluster FC configuration requires four cluster interconnect switches (if you are not using two-node switchless clusters)

These switches provide cluster communication among the controller modules in each cluster. The switches are not required if the controller modules at each site are configured as a two-node switchless cluster.

Requirement for FC-to-SAS bridges

The fabric-attached MetroCluster FC configuration requires one pair of FC-to-SAS bridges for each stack group of SAS shelves.

> FibreBridge 6500N bridges are not supported in configurations running ONTAP 9.8 and later.

- FibreBridge 7600N or 7500N bridges support up to four SAS stacks.
- FibreBridge 6500N bridges support only one SAS stack.
- Each stack can use different models of IOM.

  A mix of IOM12 modules and IOM3 modules is not supported within the same storage stack. A mix of IOM12 modules and IOM6 modules is supported within the same storage stack if your system is running a supported version of ONTAP.

  Supported IOM modules depend on the version of ONTAP you are running.

- Naming must be unique within the MetroCluster configuration.

The suggested names used as examples in this guide identify the controller module and stack that the bridge connects to, as shown below.

Pool and drive requirements (minimum supported)

Eight SAS disk shelves are recommended (four shelves at each site) to allow disk ownership on a per-shelf basis.

The MetroCluster configuration requires the minimum configuration at each site:

- Each node has at least one local pool and one remote pool at the site.

  For example, in a four-node MetroCluster configuration with two nodes at each site, four pools are required at each site.

- At least seven drives in each pool.

  In a four-node MetroCluster configuration with a single mirrored data aggregate per node, the minimum configuration requires 24 disks at the site.

In a minimum supported configuration, each pool has the following drive layout:

- Three root drives
- Three data drives
- One spare drive

In a minimum supported configuration, at least one shelf is needed per site.

MetroCluster configurations support RAID-DP and RAID4.

Drive location considerations for partially populated shelves

For correct auto-assignment of drives when using shelves that are half populated (12 drives in a 24-drive shelf), drives should be located in slots 0-5 and 18-23.

In a configuration with a partially populated shelf, the drives must be evenly distributed in the four quadrants of the shelf.

Mixing IOM12 and IOM 6 modules in a stack

Your version of ONTAP must support shelf mixing. Refer to the Interoperability Matrix Tool (IMT) to see if your version of ONTAP supports shelf mixing. NetApp Interoperability

For further details on shelf mixing see: Hot-adding shelves with IOM12 modules to a stack of shelves with IOM6 modules

Bridge naming conventions

The bridges use the following example naming:

`bridge_site_stack grouplocation in pair`

This portion of the name…	Identifies the…	Possible values…
site	Site on which the bridge pair physically resides.	A or B
stack group	Number of the stack group to which the bridge pair connects. • FibreBridge 7600N or 7500N bridges support up to four stacks in the stack group. The stack group can contain no more than 10 storage shelves. • FibreBridge 6500N bridges support only a single stack in the stack group.	1, 2, etc.
location in pair	Bridge within the bridge pair.A pair of bridges connect to a specific stack group.	a or b

Example bridge names for one stack group on each site:

- bridge_A_1a
- bridge_A_1b

- bridge_B_1a
- bridge_B_1b

Configuration worksheets for FC switches and FC-to-SAS bridges

Before beginning to configure the MetroCluster sites, you can use the following worksheets to record your site information:

Site A worksheet

Site B worksheet

Installing and cabling MetroCluster components

The storage controllers must be cabled to the FC switches and the ISLs must be cabled to link the MetroCluster sites. The storage controllers must also be cabled to the cluster peering, data, and management networks.

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 controller modules, the switch types, and the number of disk shelf stacks in your configuration.

2. Properly ground yourself.
3. Install the controller modules in the rack or cabinet.

   AFF and FAS Documentation Center

4. Install the FC switches in the rack or cabinet.
5. Install the disk shelves, power them on, and then set the shelf IDs.
   - You must power-cycle each disk shelf.
   - Shelf IDs must be unique for each SAS disk shelf within each MetroCluster DR group (including both sites).
6. 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.

The *ATTO FibreBridge Installation and Operation Manual* for your bridge model contains more information and an illustration of the installation.

> For adequate port space access and FRU serviceability, you must leave 1U space below the bridge pair and cover this space with a tool-less blanking panel.

b. Connect each bridge to a power source that provides a proper ground.

c. Power on each bridge.

> 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 new controller module's FC-VI and HBA ports to the FC switches

The FC-VI ports and HBAs (host bus adapters) must be cabled to the site FC switches on each controller module in the MetroCluster configuration.

Steps

1. Cable the FC-VI ports and HBA ports, using the table for your configuration and switch model.
   - Port assignments for FC switches when using ONTAP 9.1 and later
   - Port assignments for FC switches when using ONTAP 9.0
   - Port assignments for systems using two initiator ports

Cabling the ISLs between MetroCluster sites

You must connect the FC switches at each site through the fiber-optic Inter-Switch Links (ISLs) to form the switch fabrics that connect the MetroCluster components.

About this task

This must be done for both switch fabrics.

Steps

1. Connect the FC switches at each site to all ISLs, using the cabling in the table that corresponds to your configuration and switch model.
   - Port assignments for FC switches when using ONTAP 9.1 and later
   - Port assignments for FC switches when using ONTAP 9.0

Related information

Considerations for ISLs

Port assignments for systems using two initiator ports

You can configure FAS8020, AFF8020, FAS8200, and AFF A300 systems using a single initiator port for each fabric and two initiator ports for each controller.

You can follow the cabling for the FibreBridge 6500N bridge or FibreBridge 7500N or 7600N bridge using only one FC port (FC1 or FC2). Instead of using four initiators, connect only two initiators and leave the other two that are connected to the switch port empty.

You must apply the correct RCF file for the FibreBridge 6500N bridge's configuration.

If zoning is performed manually, then follow the zoning used for a FibreBridge 6500N or a FibreBridge 7500N or 7600N bridge using one FC port (FC1 or FC2). In this scenario, one initiator port rather than two is added to each zone member per fabric.

You can change the zoning or perform an upgrade from a FibreBridge 6500 to a FibreBridge 7500 using the procedure *Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7500N or 7600N bridge* from the MetroCluster Maintenance Guide.

The following table shows port assignments for FC switches when using ONTAP 9.1 and later.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only			
MetroCluster 1 or DR Group 1			
Component	**Port**	**Brocade switch models 6505, 6510, 6520, 7840, G620, G610, and DCX 8510-8**	
		Connects to FC switch…	**Connects to switch port…**
controller_x_1	FC-VI port a	1	0
	FC-VI port b	2	0
	FC-VI port c	1	1
	FC-VI port d	2	1
	HBA port a	1	2
	HBA port b	2	2
	HBA port c	-	-
	HBA port d	-	-
Stack 1	bridge_x_1a	1	8
	bridge_x_1b	2	8
Stack y	bridge_x_ya	1	11
	bridge_x_yb	2	11

The following table shows port assignments for FC switches when using ONTAP 9.0.

MetroCluster two-node configuration			
Component	**Port**	**Brocade 6505, 6510, or DCX 8510-8**	
		FC_switch_x_1	**FC_switch_x_2**
controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2

Port assignments for FC switches when using ONTAP 9.0

You need to verify that you are using the specified port assignments when you cable the FC switches. The port assignments are different between ONTAP 9.0 and later versions of ONTAP.

Ports that are not used for attaching initiator ports, FC-VI ports, or ISLs can be reconfigured to act as storage ports. However, if the supported RCFs are being used, the zoning must be changed accordingly.

If the supported RCF files are used, ISL ports may not connect to the same ports shown here and may need to be reconfigured manually.

Overall cabling guidelines

You should be aware of the following guidelines when using the cabling tables:

- The Brocade and Cisco switches use different port numbering:
  - On Brocade switches, the first port is numbered 0.
  - On Cisco switches, the first port is numbered 1.
- The cabling is the same for each FC switch in the switch fabric.
- AFF A300 and FAS8200 storage systems 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.

Brocade port usage for controller connections in an eight-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Brocade switches:

MetroCluster eight-node configuration			
Component	**Port**	**Brocade 6505, 6510, or DCX 8510-8**	
		FC_switch_x_1	**FC_switch_x_2**
controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2
controller_x_2	FC-VI port a	3	-
	FC-VI port b	-	3
	HBA port a	4	-
	HBA port b	-	4
	HBA port c	5	-
	HBA port d	-	5
controller_x_3	FC-VI port a	6	
	FC-VI port b	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8

controller_x_4	FC-VI port a	9	-
	FC-VI port b	-	9
	HBA port a	10	-
	HBA port b	-	10
	HBA port c	11	-
	HBA port d	-	11

Brocade port usage for FC-to-SAS bridge connections in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage when using FibreBridge 7500 bridges:

MetroCluster eight-node configuration			
FibreBridge 7500 bridge	**Port**	**Brocade 6505, 6510, or DCX 8510-8**	
		FC_switch_x_1	**FC_switch_x_2**
bridge_x_1a	FC1	12	-
	FC2	-	12
bridge_x_1b	FC1	13	-
	FC2	-	13
bridge_x_2a	FC1	14	-
	FC2	-	14
bridge_x_2b	FC1	15	-
	FC2	-	15
bridge_x_3a	FC1	16	-
	FC2	-	16
bridge_x_3b	FC1	17	-
	FC2	-	17

bridge_x_4a	FC1	18	-
	FC2	-	18
bridge_x_4b	FC1	19	-
	FC2	-	19

The following table shows bridge port usage when using FibreBridge 6500 bridges:

MetroCluster eight-node configuration			
FibreBridge 6500 bridge	**Port**	**Brocade 6505, 6510, or DCX 8510-8**	
		FC_switch_x_1	**FC_switch_x_2**
bridge_x_1a	FC1	12	-
bridge_x_1b	FC1	-	12
bridge_x_2a	FC1	13	-
bridge_x_2b	FC1	-	13
bridge_x_3a	FC1	14	-
bridge_x_3b	FC1	-	14
bridge_x_4a	FC1	15	-
bridge_x_4b	FC1	-	15
bridge_x_5a	FC1	16	-
bridge_x_5b	FC1	-	16
bridge_x_6a	FC1	17	-
bridge_x_6b	FC1	-	17
bridge_x_7a	FC1	18	-
bridge_x_7b	FC1	-	18
bridge_x_8a	FC1	19	-

bridge_x_8b	FC1	-	19

Brocade port usage for ISLs in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

MetroCluster eight-node configuration		
ISL port	**Brocade 6505, 6510, or DCX 8510-8**	
	FC_switch_x_1	**FC_switch_x_2**
ISL port 1	20	20
ISL port 2	21	21
ISL port 3	22	22
ISL port 4	23	23

Brocade port usage for controllers in a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

MetroCluster four-node configuration			
Component	**Port**	**Brocade 6505, 6510, or DCX 8510-8**	
		FC_switch_x_1	**FC_switch_x_2**
controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2

controller_x_2	FC-VI port a	3	-
	FC-VI port b	-	3
	HBA port a	4	-
	HBA port b	-	4
	HBA port c	5	-
	HBA port d	-	5

Brocade port usage for bridges in a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows bridge port usage up to port 17 when using FibreBridge 7500 bridges. Additional bridges can be cabled to ports 18 through 23.

MetroCluster four-node configuration					
FibreBridge 7500 bridge	**Port**	**Brocade 6510 or DCX 8510-8**		**Brocade 6505**	
		FC_switch_x_1	**FC_switch_x_2**	**FC_switch_x_1**	**FC_switch_x_2**
bridge_x_1a	FC1	6	-	6	-
	FC2	-	6	-	6
bridge_x_1b	FC1	7	-	7	-
	FC2	-	7	-	7
bridge_x_2a	FC1	8	-	12	-
	FC2	-	8	-	12
bridge_x_2b	FC1	9	-	13	-
	FC2	-	9	-	13
bridge_x_3a	FC1	10	-	14	-
	FC2	-	10	-	14

bridge_x_3b	FC1	11	-	15	-
	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
	FC2	-	12	-	16
bridge_x_4b	FC1	13	-	17	-
	FC2	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

The following table shows bridge port usage when using FibreBridge 6500 bridges:

MetroCluster four-node configuration					
FibreBridge 6500 bridge	**Port**	**Brocade 6510, DCX 8510-8**		**Brocade 6505**	
		FC_switch_x_1	**FC_switch_x_2**	**FC_switch_x_1**	**FC_switch_x_2**
bridge_x_1a	FC1	6	-	6	-
bridge_x_1b	FC1	-	6	-	6
bridge_x_2a	FC1	7	-	7	-
bridge_x_2b	FC1	-	7	-	7
bridge_x_3a	FC1	8	-	12	-
bridge_x_3b	FC1	-	8	-	12
bridge_x_4a	FC1	9	-	13	-
bridge_x_4b	FC1	-	9	-	13
bridge_x_5a	FC1	10	-	14	-
bridge_x_5b	FC1	-	10	-	14
bridge_x_6a	FC1	11	-	15	-

bridge_x_6b	FC1	-	11	-	15
bridge_x_7a	FC1	12	-	16	-
bridge_x_7b	FC1	-	12	-	16
bridge_x_8a	FC1	13	-	17	-
bridge_x_8b	FC1	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

Brocade port usage for ISLs in a four-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

MetroCluster four-node configuration				
ISL port	**Brocade 6510, DCX 8510-8**		**Brocade 6505**	
	FC_switch_x_1	**FC_switch_x_2**	**FC_switch_x_1**	**FC_switch_x_2**
ISL port 1	20	20	8	8
ISL port 2	21	21	9	9
ISL port 3	22	22	10	10
ISL port 4	23	23	11	11

Brocade port usage for controllers in a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

MetroCluster two-node configuration			
Component	**Port**	**Brocade 6505, 6510, or DCX 8510-8**	
		FC_switch_x_1	**FC_switch_x_2**

controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2

Brocade port usage for bridges in a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows bridge port usage up to port 17 when using FibreBridge 7500 bridges. Additional bridges can be cabled to ports 18 through 23.

MetroCluster two-node configuration					
FibreBridge 7500 bridge	**Port**	**Brocade 6510, DCX 8510-8**		**Brocade 6505**	
		FC_switch_x_1	**FC_switch_x_2**	**FC_switch_x_1**	**FC_switch_x_2**
bridge_x_1a	FC1	6	-	6	-
	FC2	-	6	-	6
bridge_x_1b	FC1	7	-	7	-
	FC2	-	7	-	7
bridge_x_2a	FC1	8	-	12	-
	FC2	-	8	-	12
bridge_x_2b	FC1	9	-	13	-
	FC2	-	9	-	13
bridge_x_3a	FC1	10	-	14	-
	FC2	-	10	-	14

bridge_x_3b	FC1	11	-	15	-
	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
	FC2	-	12	-	16
bridge_x_4b	FC1	13	-	17	-
	FC2	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

The following table shows bridge port usage when using FibreBridge 6500 bridges:

MetroCluster two-node configuration					
FibreBridge 6500 bridge	**Port**	**Brocade 6510, DCX 8510-8**		**Brocade 6505**	
		FC_switch_x_1	**FC_switch_x_2**	**FC_switch_x_1**	**FC_switch_x_2**
bridge_x_1a	FC1	6	-	6	-
bridge_x_1b	FC1	-	6	-	6
bridge_x_2a	FC1	7	-	7	-
bridge_x_2b	FC1	-	7	-	7
bridge_x_3a	FC1	8	-	12	-
bridge_x_3b	FC1	-	8	-	12
bridge_x_4a	FC1	9	-	13	-
bridge_x_4b	FC1	-	9	-	13
bridge_x_5a	FC1	10	-	14	-
bridge_x_5b	FC1	-	10	-	14
bridge_x_6a	FC1	11	-	15	-

bridge_x_6b	FC1	-	11	-	15
bridge_x_7a	FC1	12	-	16	-
bridge_x_7b	FC1	-	12	-	16
bridge_x_8a	FC1	13	-	17	-
bridge_x_8b	FC1	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

Brocade port usage for ISLs in a two-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

MetroCluster two-node configuration				
ISL port	**Brocade 6510, DCX 8510-8**		**Brocade 6505**	
	FC_switch_x_1	**FC_switch_x_2**	**FC_switch_x_1**	**FC_switch_x_2**
ISL port 1	20	20	8	8
ISL port 2	21	21	9	9
ISL port 3	22	22	10	10
ISL port 4	23	23	11	11

Cisco port usage for controllers in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows controller port usage on Cisco switches:

MetroCluster eight-node configuration			
Component	**Port**	**Cisco 9148 or 9148S**	
		FC_switch_x_1	**FC_switch_x_2**

controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3
controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	HBA port a	5	-
	HBA port b	-	5
	HBA port c	6	-
	HBA port d	-	6
controller_x_3	FC-VI port a	7	
	FC-VI port b	-	7
	HBA port a	8	-
	HBA port b	-	8
	HBA port c	9	-
	HBA port d	-	9

controller_x_4	FC-VI port a	10	-
	FC-VI port b	-	10
	HBA port a	11	-
	HBA port b	-	11
	HBA port c	13	-
	HBA port d	-	13

Cisco port usage for FC-to-SAS bridges in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage up to port 23 when using FibreBridge 7500 bridges. Additional bridges can be attached using ports 25 through 48.

MetroCluster eight-node configuration			
FibreBridge 7500 bridge	**Port**	**Cisco 9148 or 9148S**	
		FC_switch_x_1	**FC_switch_x_2**
bridge_x_1a	FC1	14	14
	FC2	-	-
bridge_x_1b	FC1	15	15
	FC2	-	-
bridge_x_2a	FC1	17	17
	FC2	-	-
bridge_x_2b	FC1	18	18
	FC2	-	-
bridge_x_3a	FC1	19	19
	FC2	-	-
bridge_x_3b	FC1	21	21
	FC2	-	-

bridge_x_4a	FC1	22	22
	FC2	-	-
bridge_x_4b	FC1	23	23
	FC2	-	-
Additional bridges can be attached using ports 25 through 48 following the same pattern.			

The following table shows bridge port usage up to port 23 when using FibreBridge 6500 bridges. Additional bridges can be attached using ports 25-48.

MetroCluster eight node			
FibreBridge 6500 bridge	**Port**	**Cisco 9148 or 9148S**	
		FC_switch_x_1	**FC_switch_x_2**
bridge_x_1a	FC1	14	-
bridge_x_1b	FC1	-	14
bridge_x_2a	FC1	15	-
bridge_x_2b	FC1	-	15
bridge_x_3a	FC1	17	-
bridge_x_3b	FC1	-	17
bridge_x_4a	FC1	18	-
bridge_x_4b	FC1	-	18
bridge_x_5a	FC1	19	-
bridge_x_5b	FC1	-	19
bridge_x_6a	FC1	21	-
bridge_x_6b	FC1	-	21
bridge_x_7a	FC1	22	-
bridge_x_7b	FC1	-	22

bridge_x_8a	FC1	23	-
bridge_x_8b	FC1	-	23
Additional bridges can be attached using ports 25 through 48 following the same pattern.			

Cisco port usage for ISLs in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

MetroCluster eight-node configuration		
ISL port	**Cisco 9148 or 9148S**	
	FC_switch_x_1	**FC_switch_x_2**
ISL port 1	12	12
ISL port 2	16	16
ISL port 3	20	20
ISL port 4	24	24

Cisco port usage for controllers in a four-node MetroCluster configuration

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Cisco switches:

MetroCluster four-node configuration			
Component	**Port**	**Cisco 9148, 9148S, or 9250i**	
		FC_switch_x_1	**FC_switch_x_2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3

controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	HBA port a	5	-
	HBA port b	-	5
	HBA port c	6	-
	HBA port d	-	6

Cisco port usage for FC-to-SAS bridges in a four-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage up to port 14 when using FibreBridge 7500 bridges. Additional bridges can be attached to ports 15 through 32 following the same pattern.

MetroCluster four-node configuration			
FibreBridge 7500 bridge	**Port**	**Cisco 9148, 9148S, or 9250i**	
		FC_switch_x_1	**FC_switch_x_2**
bridge_x_1a	FC1	7	-
	FC2	-	7
bridge_x_1b	FC1	8	-
	FC2	-	8
bridge_x_2a	FC1	9	-
	FC2	-	9
bridge_x_2b	FC1	10	-
	FC2	-	10
bridge_x_3a	FC1	11	-
	FC2	-	11
bridge_x_3b	FC1	12	-
	FC2	-	12

bridge_x_4a	FC1	13	-
	FC2	-	13
bridge_x_4b	FC1	14	-
	FC2	-	14

The following table shows bridge port usage when using FibreBridge 6500 bridges up to port 14. Additional bridges can be attached to ports 15 through 32 following the same pattern.

MetroCluster four-node configuration			
FibreBridge 6500 bridge	**Port**	**Cisco 9148, 9148S, or 9250i**	
		FC_switch_x_1	**FC_switch_x_2**
bridge_x_1a	FC1	7	-
bridge_x_1b	FC1	-	7
bridge_x_2a	FC1	8	-
bridge_x_2b	FC1	-	8
bridge_x_3a	FC1	9	-
bridge_x_3b	FC1	-	9
bridge_x_4a	FC1	10	-
bridge_x_4b	FC1	-	10
bridge_x_5a	FC1	11	-
bridge_x_5b	FC1	-	11
bridge_x_6a	FC1	12	-
bridge_x_6b	FC1	-	12
bridge_x_7a	FC1	13	-
bridge_x_7b	FC1	-	13
bridge_x_8a	FC1	14	-

bridge_x_8b	FC1	-	14
Additional bridges can be attached to ports 15 through 32 following the same pattern.			

Cisco 9148 and 9148S port usage for ISLs on a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows ISL port usage:

MetroCluster four-node configuration		
ISL port	**Cisco 9148 or 9148S**	
	FC_switch_x_1	**FC_switch_x_2**
ISL port 1	36	36
ISL port 2	40	40
ISL port 3	44	44
ISL port 4	48	48

Cisco 9250i port usage for ISLs on a four-node MetroCluster configuration running ONTAP 9.0

The Cisco 9250i switch uses the FCIP ports for the ISL.

Ports 40 through 48 are 10 GbE ports and are not used in the MetroCluster configuration.

Cisco port usage for controllers in a two-node MetroCluster configuration

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Cisco switches:

MetroCluster two-node configuration			
Component	**Port**	**Cisco 9148, 9148S, or 9250i**	
		FC_switch_x_1	**FC_switch_x_2**

controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3

Cisco port usage for FC-to-SAS bridges in a two-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage up to port 14 when using FibreBridge 7500 bridges. Additional bridges can be attached to ports 15 through 32 following the same pattern.

MetroCluster two-node configuration			
FibreBridge 7500 bridge	**Port**	**Cisco 9148, 9148S, or 9250i**	
		FC_switch_x_1	**FC_switch_x_2**
bridge_x_1a	FC1	7	-
	FC2	-	7
bridge_x_1b	FC1	8	-
	FC2	-	8
bridge_x_2a	FC1	9	-
	FC2	-	9
bridge_x_2b	FC1	10	-
	FC2	-	10
bridge_x_3a	FC1	11	-
	FC2	-	11
bridge_x_3b	FC1	12	-
	FC2	-	12

bridge_x_4a	FC1	13	-
	FC2	-	13
bridge_x_4b	FC1	14	-
	FC2	-	14

The following table shows bridge port usage when using FibreBridge 6500 bridges up to port 14. Additional bridges can be attached to ports 15 through 32 following the same pattern.

MetroCluster two-node configuration			
FibreBridge 6500 bridge	**Port**	**Cisco 9148, 9148S, or 9250i**	
		FC_switch_x_1	**FC_switch_x_2**
bridge_x_1a	FC1	7	-
bridge_x_1b	FC1	-	7
bridge_x_2a	FC1	8	-
bridge_x_2b	FC1	-	8
bridge_x_3a	FC1	9	-
bridge_x_3b	FC1	-	9
bridge_x_4a	FC1	10	-
bridge_x_4b	FC1	-	10
bridge_x_5a	FC1	11	-
bridge_x_5b	FC1	-	11
bridge_x_6a	FC1	12	-
bridge_x_6b	FC1	-	12
bridge_x_7a	FC1	13	-
bridge_x_7b	FC1	-	13
bridge_x_8a	FC1	14	-

bridge_x_8b	FC1	-	14
Additional bridges can be attached to ports 15 through 32 following the same pattern.			

Cisco 9148 or 9148S port usage for ISLs on a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows ISL port usage:

MetroCluster two-node configuration		
ISL port	**Cisco 9148 or 9148S**	
	FC_switch_x_1	**FC_switch_x_2**
ISL port 1	36	36
ISL port 2	40	40
ISL port 3	44	44
ISL port 4	48	48

Cisco 9250i port usage for ISLs on a two-node MetroCluster configuration running ONTAP 9.0

The Cisco 9250i switch uses the FCIP ports for the ISL.

Ports 40 through 48 are 10 GbE ports and are not used in the MetroCluster configuration.

Port assignments for FC switches when using ONTAP 9.1 or later

You need to verify that you are using the specified port assignments when you cable the FC switches when using ONTAP 9.1 and later.

Ports that are not used for attaching initiator ports, FC-VI ports, or ISLs can be reconfigured to act as storage ports. However, if the supported RCFs are being used, the zoning must be changed accordingly.

If the supported RCFs are used, ISL ports might not connect to the same ports shown and might need to be reconfigured manually.

If you configured your switches using the port assignments for ONTAP 9, you can continue to use the older assignments. However, new configurations running ONTAP 9.1 or later releases should use the port assignments shown here.

Overall cabling guidelines

You should be aware of the following guidelines when using the cabling tables:

- The Brocade and Cisco switches use different port numbering:
  - On Brocade switches, the first port is numbered 0.

    ◦ On Cisco switches, the first port is numbered 1.

- The cabling is the same for each FC switch in the switch fabric.
- AFF A300 and FAS8200 storage systems 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 require four FC-VI ports. The following tables show cabling for the FC switches with four FC-VI ports on each controller except for the Cisco 9250i switch.

  For other storage systems, use the cabling shown in the tables but ignore the cabling for FC-VI ports c and d.

  You can leave those ports empty.
- AFF A400 and FAS8300 storage systems use ports 2a and 2b for FC-VI connectivity.
- If you have two MetroCluster configurations sharing ISLs, use the same port assignments as that for an eight-node MetroCluster cabling.

  The number of ISLs you cable may vary depending on site's requirements.

  See the section on ISL considerations.

Brocade port usage for controllers in a MetroCluster configuration running ONTAP 9.1 or later

The following tables show port usage on Brocade switches. The tables show the maximum supported configuration, with eight controller modules in two DR groups. For smaller configurations, ignore the rows for the additional controller modules. Note that eight ISLs are supported only on the Brocade 6510, Brocade DCX 8510-8, G620, G630, G620-1, G630-1, and G720 switches.

> - Port usage for the Brocade 6505 and Brocade G610 switches in an eight-node MetroCluster configuration is not shown. Due to the limited number of ports, port assignments must be made on a site-by-site basis depending on the controller module model and the number of ISLs and bridge pairs in use.
> - The Brocade DCX 8510-8 switch can use the same port layout as the 6510 switch ***or*** the 7840 switch.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only				
MetroCluster 1 or DR Group 1				
Component	**Port**	**Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 and DCX 8510-8**		**Brocade switch model G720**
		Connects to FC switch…	**Connects to switch port…**	**Connects to switch port…**

controller_x_1	FC-VI port a	1	0	0
	FC-VI port b	2	0	0
	FC-VI port c	1	1	1
	FC-VI port d	2	1	1
	HBA port a	1	2	8
	HBA port b	2	2	8
	HBA port c	1	3	9
	HBA port d	2	3	9
controller_x_2	FC-VI port a	1	4	4
	FC-VI port b	2	4	4
	FC-VI port c	1	5	5
	FC-VI port d	2	5	5
	HBA port a	1	6	12
	HBA port b	2	6	12
	HBA port c	1	7	13
	HBA port d	2	7	13

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only				
MetroCluster 1 or DR Group 1				
Component	**Port**	**Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 and DCX 8510-8**		**Brocade switch model G720**
		Connects to FC switch…	**Connects to switch port…**	**Connects to switch port…**
Stack 1	bridge_x_1a	1	8	10
	bridge_x_1b	2	8	10

Stack 2	bridge_x_2a	1	9	11
	bridge_x_2b	2	9	11
Stack 3	bridge_x_3a	1	10	14
	bridge_x_4b	2	10	14
Stack y	bridge_x_ya	1	11	15
	bridge_x_yb	2	11	15

- On G620, G630, G620-1 and G630-1 switches, additional bridges can be cabled to ports 12 - 17, 20 and 21.
- On G610 switches, additional bridges can be cabled to ports 12 - 19.
- On G720 switches, additional bridges can be cabled to ports 16 - 17, 20 and 21.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only							
MetroCluster 2 or DR Group 2							
			Brocade switch model				
Component	**Port**	**Connects to FC_switch …**	**6510, DCX 8510-8**	**6520**	**7840, DCX 8510-8**	**G620, G620-1, G630, G630-1**	**G720**
controller_x_3	FC-VI port a	1	24	48	12	18	18
	FC-VI port b	2	24	48	12	18	18
	FC-VI port c	1	25	49	13	19	19
	FC-VI port d	2	25	49	13	19	19
	HBA port a	1	26	50	14	24	26
	HBA port b	2	26	50	14	24	26
	HBA port c	1	27	51	15	25	27
	HBA port d	2	27	51	15	25	27

controller_x_4	FC-VI port a	1	28	52	16	22	22
	FC-VI port b	2	28	52	16	22	22
	FC-VI port c	1	29	53	17	23	23
	FC-VI port d	2	29	53	17	23	23
	HBA port a	1	30	54	18	28	30
	HBA port b	2	30	54	18	28	30
	HBA port c	1	31	55	19	29	31
	HBA port d	2	32	55	19	29	31
Stack 1	bridge_x_51a	1	32	56	20	26	32
	bridge_x_51b	2	32	56	20	26	32
Stack 2	bridge_x_52a	1	33	57	21	27	33
	bridge_x_52b	2	33	57	21	27	33
Stack 3	bridge_x_53a	1	34	58	22	30	34
	bridge_x_54b	2	34	58	22	30	34
Stack y	bridge_x_ya	1	35	59	23	31	35
	bridge_x_yb	2	35	59	23	31	35

- On G720 switches, additional bridges can be cabled to ports 36-39.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)
MetroCluster 1 or DR Group 1

Component		Port	Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1, and DCX 8510-8		Brocade switch G720
			Connects to FC_switch…	Connects to switch port…	Connects to switch port…
Stack 1	bridge_x_1a	FC1	1	8	10
		FC2	2	8	10
	bridge_x_1B	FC1	1	9	11
		FC2	2	9	11
Stack 2	bridge_x_2a	FC1	1	10	14
		FC2	2	10	14
	bridge_x_2B	FC1	1	11	15
		FC2	2	11	15
Stack 3	bridge_x_3a	FC1	1	12*	16
		FC2	2	12*	16
	bridge_x_3B	FC1	1	13*	17
		FC2	2	13*	17
Stack y	bridge_x_ya	FC1	1	14*	20
		FC2	2	14*	20
	bridge_x_yb	FC1	1	15*	21
		FC2	2	15*	21

* Ports 12 through 15 are reserved for the second MetroCluster or DR group on the Brocade 7840 switch.

> ⓘ Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620, G630, G620-1 and G630-1 switches.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

MetroCluster 2 or DR Group 2							
Component	**Port**	**Brocade switch model**					
		Connects to FC_switch…	**6510, DCX 8510-8**	**6520**	**7840, DCX 8510-8**	**G620, G620-1, G630, G630-1**	**G720**
controller_x_3	FC-VI port a	1	24	48	12	18	18
	FC-VI port b	2	24	48	12	18	18
	FC-VI port c	1	25	49	13	19	19
	FC-VI port d	2	25	49	13	19	19
	HBA port a	1	26	50	14	24	26
	HBA port b	2	26	50	14	24	26
	HBA port c	1	27	51	15	25	27
	HBA port d	2	27	51	15	25	27

controller_x_4		FC-VI port a	1	28	52	16	22	22
		FC-VI port b	2	28	52	16	22	22
		FC-VI port c	1	29	53	17	23	23
		FC-VI port d	2	29	53	17	23	23
		HBA port a	1	30	54	18	28	30
		HBA port b	2	30	54	18	28	30
		HBA port c	1	31	55	19	29	31
		HBA port d	2	31	55	19	29	31
Stack 1	bridge_x_51a	FC1	1	32	56	20	26	32
		FC2	2	32	56	20	26	32
	bridge_x_51b	FC1	1	33	57	21	27	33
		FC2	2	33	57	21	27	33
Stack 2	bridge_x_52a	FC1	1	34	58	22	30	34
		FC2	2	34	58	22	30	34
	bridge_x_52b	FC1	1	35	59	23	31	35
		FC2	2	35	59	23	31	35

Stack 3	bridge_x_ 53a	FC1	1	36	60	-	32	36
		FC2	2	36	60	-	32	36
	bridge_x_ 53b	FC1	1	37	61	-	33	37
		FC2	2	37	61	-	33	37
Stack y	bridge_x_ 5ya	FC1	1	38	62	-	34	38
		FC2	2	38	62	-	34	38
	bridge_x_ 5yb	FC1	1	39	63	-	35	39
		FC2	2	39	63	-	35	39

> Additional bridges can be cabled to ports 36 to 39 in G620, G630, G620-1, and G630-1 switches.

Brocade port usage for ISLs in a MetroCluster configuration running ONTAP 9.1 or later

The following table shows ISL port usage for the Brocade switches.

> AFF A700 or FAS9000 systems support up to eight ISLs for improved performance. Eight ISLs are supported on the Brocade 6510 and G620 switches.

Switch model	ISL port	Switch port
Brocade 6520	ISL port 1	23
	ISL port 2	47
	ISL port 3	71
	ISL port 4	95
Brocade 6505	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23

Switch model	ISL port	Switch port
Brocade 6510 and Brocade DCX 8510-8	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47
Brocade 7810	ISL port 1	ge2 (10-Gbps)
	ISL port 2	ge3(10-Gbps)
	ISL port 3	ge4 (10-Gbps)
	ISL port 4	ge5 (10-Gbps)
	ISL port 5	ge6 (10-Gbps)
	ISL port 6	ge7 (10-Gbps)
Brocade 7840 **Note**: The Brocade 7840 switch supports either two 40 Gbps VE-ports or up to four 10 Gbps VE-ports per switch for the creation of FCIP ISLs.	ISL port 1	ge0 (40-Gbps) or ge2 (10-Gbps)
	ISL port 2	ge1 (40-Gbps) or ge3 (10-Gbps)
	ISL port 3	ge10 (10-Gbps)
	ISL port 4	ge11 (10-Gbps)
Brocade G610	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23

Switch model	ISL port	Switch port
Brocade G620, G620-1, G630, G630-1, G720	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47

Cisco port usage for controllers in a MetroCluster configuration running ONTAP 9.4 or later

The tables show the maximum supported configurations, with eight controller modules in two DR groups. For smaller configurations, ignore the rows for the additional controller modules.

Cisco 9396S			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	
	HBA port d	-	8
controller_x_3	FC-VI port a	49	
	FC-VI port b	-	49
	FC-VI port c	50	-
	FC-VI port d	-	50
	HBA port a	51	-
	HBA port b	-	51
	HBA port c	52	
	HBA port d	-	52

controller_x_4	FC-VI port a	53	-
	FC-VI port b	-	53
	FC-VI port c	54	-
	FC-VI port d	-	54
	HBA port a	55	-
	HBA port b	-	55
	HBA port c	56	-
	HBA port d	-	56

Cisco 9148S			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8
controller_x_3	FC-VI port a	25	
	FC-VI port b	-	25
	FC-VI port c	26	-
	FC-VI port d	-	26
	HBA port a	27	-
	HBA port b	-	27
	HBA port c	28	-
	HBA port d	-	28

controller_x_4	FC-VI port a	29	-
	FC-VI port b	-	29
	FC-VI port c	30	-
	FC-VI port d	-	30
	HBA port a	31	-
	HBA port b	-	31
	HBA port c	32	-
	HBA port d	-	32

Cisco 9132T			
MDS module 1			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8
MDS module 2			
Component	Port	Switch 1	Switch 2
controller_x_3	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_4	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8

The following table shows systems with two FC-VI ports. AFF A700 and FAS9000 systems have four FC-VI ports (a, b, c, and d). If using an AFF A700 or FAS9000 system, the port assignments move along by one position. For example, FC-VI ports c and d go to switch port 2 and HBA ports a and b go to switch port 3.

Cisco 9250i **Note: The Cisco 9250i switch is not supported for eight-node MetroCluster configurations.**			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3

controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	HBA port a	5	-
	HBA port b	-	5
	HBA port c	6	-
	HBA port d	-	6
controller_x_3	FC-VI port a	7	-
	FC-VI port b	-	7
	HBA port a	8	-
	HBA port b	-	8
	HBA port c	9	-
	HBA port d	-	9
controller_x_4	FC-VI port a	10	-
	FC-VI port b	-	10
	HBA port a	11	-
	HBA port b	-	11
	HBA port c	13	-
	HBA port d	-	13

Cisco port usage for FC-to-SAS bridges in a MetroCluster configuration running ONTAP 9.1 or later

Cisco 9396S			
FibreBridge 7500 using two FC ports	**Port**	**Switch 1**	**Switch 2**

bridge_x_1a	FC1	9	-
	FC2	-	9
bridge_x_1b	FC1	10	-
	FC2	-	10
bridge_x_2a	FC1	11	-
	FC2	-	11
bridge_x_2b	FC1	12	-
	FC2	-	12
bridge_x_3a	FC1	13	-
	FC2	-	13
bridge_x_3b	FC1	14	-
	FC2	-	14
bridge_x_4a	FC1	15	-
	FC2	-	15
bridge_x_4b	FC1	16	-
	FC2	-	16

Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.

Cisco 9148S			
FibreBridge 7500 using two FC ports	**Port**	**Switch 1**	**Switch 2**
bridge_x_1a	FC1	9	-
	FC2	-	9

bridge_x_1b	FC1	10	-
	FC2	-	10
bridge_x_2a	FC1	11	-
	FC2	-	11
bridge_x_2b	FC1	12	-
	FC2	-	12
bridge_x_3a	FC1	13	-
	FC2	-	13
bridge_x_3b	FC1	14	-
	FC2	-	14
bridge_x_4a	FC1	15	-
	FC2	-	15
bridge_x_4b	FC1	16	-
	FC2	-	16

Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 33 through 40 following the same pattern.

Cisco 9132T			
FibreBridge 7500 using two FC ports	**Port**	**Switch**	**Switch 2**
bridge_x_1a	FC1	9	-
	FC2	-	9
bridge_x_1b	FC1	10	-
	FC2	-	10

bridge_x_2a	FC1	11	-
	FC2	-	11
bridge_x_2b	FC1	12	-
	FC2	-	12

Additional bridges for a second DR group or second MetroCluster configuration can be attached using the same port numbers on the second MDS module.

Cisco 9250i			
FibreBridge 7500 using two FC ports	**Port**	**Switch 1**	**Switch 2**
bridge_x_1a	FC1	14	-
	FC2	-	14
bridge_x_1b	FC1	15	-
	FC2	-	15
bridge_x_2a	FC1	17	-
	FC2	-	17
bridge_x_2b	FC1	18	-
	FC2	-	18
bridge_x_3a	FC1	19	-
	FC2	-	19
bridge_x_3b	FC1	21	-
	FC2	-	21
bridge_x_4a	FC1	22	-
	FC2	-	22

bridge_x_4b	FC1	23	-
	FC2	-	23

Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 25 through 48 following the same pattern.

The following tables show bridge port usage when using FibreBridge 6500 bridges or FibreBridge 7500 bridges using one FC port (FC1 or FC2) only. For FibreBridge 7500 bridges using one FC port, either FC1 or FC2 can be cabled to the port indicated as FC1. Additional bridges can be attached using ports 25-48.

FibreBridge 6500 bridges or FibreBridge 7500 bridges using one FC port			
FibreBridge 6500 bridge or FibreBridge 7500 using one FC port	**Port**	**Cisco 9396S**	
		Switch 1	**Switch 2**
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-

bridge_x_8b	FC1	-	16

Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.

FibreBridge 6500 bridges or FibreBridge 7500 bridges using one FC port			
Bridge	**Port**	**Cisco 9148S**	
		Switch 1	**Switch 2**
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-
bridge_x_8b	FC1	-	16

Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 25 through 48 following the same pattern.

Cisco 9250i

FibreBridge 6500 bridge or FibreBridge 7500 using one FC port	Port	Switch 1	Switch 2
bridge_x_1a	FC1	14	-
bridge_x_1b	FC1	-	14
bridge_x_2a	FC1	15	-
bridge_x_2b	FC1	-	15
bridge_x_3a	FC1	17	-
bridge_x_3b	FC1	-	17
bridge_x_4a	FC1	18	-
bridge_x_4b	FC1	-	18
bridge_x_5a	FC1	19	-
bridge_x_5b	FC1	-	19
bridge_x_6a	FC1	21	-
bridge_x_6b	FC1	-	21
bridge_x_7a	FC1	22	-
bridge_x_7b	FC1	-	22
bridge_x_8a	FC1	23	-
bridge_x_8b	FC1	-	23

Additional bridges can be attached using ports 25 through 48 following the same pattern.

Cisco port usage for ISLs in an eight-node configuration in a MetroCluster configuration running ONTAP 9.1 or later

The following table shows ISL port usage. ISL port usage is the same on all switches in the configuration.

Switch model	ISL port	Switch port

Cisco 9396S	ISL 1	44
	ISL 2	48
	ISL 3	92
	ISL 4	96
Cisco 9250i with 24 port license	ISL 1	12
	ISL 2	16
	ISL 3	20
	ISL 4	24
Cisco 9148S	ISL 1	20
	ISL 2	24
	ISL 3	44
	ISL 4	48
Cisco 9132T	ISL 1	MDS module 1 port 13
	ISL 2	MDS module 1 port 14
	ISL 3	MDS module 1 port 15
	ISL 4	MDS module 1 port 16

Cabling the cluster interconnect in eight- or four-node configurations

In eight- or four-node MetroCluster configurations, you must cable the cluster interconnect between the local controller modules at each site.

About this task

This task is not required on two-node MetroCluster configurations.

This task must be performed at both MetroCluster sites.

Step

1. Cable the cluster interconnect from one controller module to the other, or if cluster interconnect switches are used, from each controller module to the switches.

Related information

[AFF and FAS Documentation Center]

[Network and LIF management]

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.

Related information

[Cluster and SVM peering express configuration]

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.

[Considerations for configuring cluster peering]

Cabling the HA interconnect

If you have an eight- or a four-node MetroCluster configuration and the storage controllers within the HA pairs are in separate chassis, you must cable the HA interconnect between the controllers.

About this task

- This task does not apply to two-node MetroCluster configurations.
- This task must be performed at both MetroCluster sites.
- The HA interconnect must be cabled only if the storage controllers within the HA pair are in separate chassis.

  Some storage controller models support two controllers in a single chassis, in which case they use an internal HA interconnect.

Steps

1. Cable the HA interconnect if the storage controller’s HA partner is in a separate chassis.

AFF and FAS Documentation Center

2. If the MetroCluster site includes two HA pairs, repeat the previous steps on the second HA pair.
3. Repeat this task at the MetroCluster partner site.

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

Configuring the FC switches

For fabric-attached MetroCluster systems that were not pre-configured in the factory, you must configure each FC switch in the DR group. This is done manually, or, depending on the switch, can optionally be done with a configuration file.

For new systems, the FC switch fabrics are typically configured for two ISLs and do not require additional configuration unless you want to change the pre-configured IP addresses.

Configuring Brocade FC switches with RCF files

To configure a Brocade FC switch, you must reset the switch settings to factory defaults, install the switch software, and download and apply the reference configuration (RCF) files that provide the complete switch settings for certain configurations.

Before you begin

You must have access to an FTP server. The switches must have connectivity with the FTP server.

About this task

Each configuration file is different and must be used with the correct switch. Only one of the configuration files for each switch fabric contains zoning commands.

Resetting the Brocade FC switch to factory defaults

Before installing a new software version and RCF files, you must erase the current switch configuration and perform basic configuration.

About this task

You must repeat these steps on each of the FC switches in the MetroCluster fabric configuration.

Steps

1. Log in to the switch as an administrator.
2. Disable the Brocade Virtual Fabrics (VF) feature:

   `fosconfig options`

   ```
   FC_switch_A_1:admin> fosconfig --disable vf
   WARNING:  This is a disruptive operation that requires a reboot to take
   effect.
   Would you like to continue  [Y/N]: y
   ```

3. Disconnect the ISL cables from the ports on the switch.
4. Disable the switch:

   `switchcfgpersistentdisable`

   ```
   FC_switch_A_1:admin> switchcfgpersistentdisable
   ```

5. Disable the configuration:

   `cfgDisable`

   ```
   FC_switch_A_1:admin> cfgDisable
   You are about to disable zoning configuration. This action will disable
   any previous zoning configuration enabled.
   Do you want to disable zoning configuration? (yes, y, no, n): [no] y
   Updating flash ...
   Effective configuration is empty. "No  Access" default zone mode is ON.
   ```

6. Clear the configuration:

   `cfgClear`

   ```
   FC_switch_A_1:admin> cfgClear
   The Clear All action will clear all Aliases, Zones, FA Zones
   and configurations in the Defined configuration.
   Run cfgSave to commit the transaction or cfgTransAbort to
   cancel the transaction.
   Do you really want to clear all configurations?  (yes, y, no, n): [no] y
   ```

7. Save the configuration:

   `cfgSave`

```
FC_switch_A_1:admin> cfgSave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Do you want to save the Defined zoning configuration only?  (yes, y, no,
n): [no] y
Updating flash ...
```

8. Set the default configuration:

   `configDefault`

```
FC_switch_A_1:admin> configDefault
WARNING:  This is a disruptive operation that requires a switch reboot.
Would you like to continue [Y/N]: y
Executing configdefault...Please wait
2020/10/05-08:04:08, [FCR-1069], 1016, FID 128, INFO, FC_switch_A_1, The
FC Routing service is enabled.
2020/10/05-08:04:08, [FCR-1068], 1017, FID 128, INFO, FC_switch_A_1, The
FC Routing service is disabled.
2020/10/05-08:04:08, [FCR-1070], 1018, FID 128, INFO, FC_switch_A_1, The
FC Routing configuration is set to default.
Committing configuration ... done.
2020/10/05-08:04:12, [MAPS-1113], 1019, FID 128, INFO, FC_switch_A_1,
Policy dflt_conservative_policy activated.
2020/10/05-08:04:12, [MAPS-1145], 1020, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for E-Ports.
2020/10/05-08:04:12, [MAPS-1144], 1021, FID 128, INFO, FC_switch_A_1,
FPI Profile dflt_fpi_profile is activated for F-Ports.
The switch has to be rebooted to allow the changes to take effect.
2020/10/05-08:04:12, [CONF-1031], 1022, FID 128, INFO, FC_switch_A_1,
configDefault completed successfully for switch.
```

9. Set the port configuration to default for all ports:

   `portcfgdefault` *`port-number`*

```
FC_switch_A_1:admin> portcfgdefault <port number>
```

   You must complete this step for each port.

10. Verify that the switch is using the dynamic Port on Demand (POD) method.

    For Brocade Fabric OS versions before 8.0, you run the following commands as admin, and for versions 8.0 and later, you run them as root.

a. Run the license command:

`licenseport --show`

```
FC_switch_A_1:admin> licenseport -show
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

b. Enable the root user if it is disabled by Brocade.

```
FC_switch_A_1:admin> userconfig --change root -e yes
FC_switch_A_1:admin> rootaccess --set consoleonly
```

c. Run the license command:

`licenseport --show`

```
FC_switch_A_1:root> licenseport -show
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

d. Change the license method to dynamic:

`licenseport --method dynamic`

> ⓘ If the dynamic POD method is not in use (if POD method is in static) you must change the license assignment method to dynamic. Skip this step if the dynamic POD method is in use.

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

11. Reboot the switch:

`fastBoot`

```
FC_switch_A_1:admin> fastboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
```

12. Confirm that the default settings have been implemented:

    `switchShow`

13. Verify that the IP address is set correctly:

    `ipAddrShow`

    You can set the IP address with the following command, if required:

    `ipAddrSet`

Downloading the Brocade FC switch RCF file

You must download the reference configuration (RCF) file to each switch in the MetroCluster fabric configuration.

About this task

To use these RCF files, the system must be running ONTAP 9.1 or later and you must use the port layout for ONTAP 9.1 or later.

If you are planning to use only one of the FC ports on the FibreBridge bridges, configure the back-end fibre channel switches manually using the instructions found in the section, Port assignments for FC switches when using ONTAP 9.1 and later.

Steps

1. Refer to the RCF file table on the Brocade RCF download page and identify the correct RCF file for each switch in your configuration.

   The RCF files must be applied to the correct switches.

2. Download the RCF files for the switches from the MetroCluster RCF download page.

   The files must be placed in a location where they can be transferred to the switch. There is a separate file for each of the four switches that make up the two-switch fabric.

3. Repeat these steps on each switch in the configuration.

Installing the Brocade FC switch RCF file

When you configure a Brocade FC switch, you can install the switch configuration files that provide the complete switch settings for certain configurations.

About this task

These steps must be repeated on each of the Brocade FC switches in the MetroCluster fabric configuration.

Steps

1. Initiate the download and configuration process:

   `configDownload`

   Respond to the prompts as shown in the following example.

   ```
   FC_switch_A_1:admin> configDownload
   Protocol (scp, ftp, sftp, local) [ftp]:
   Server Name or IP Address [host]: <user input>
   User Name [user]:<user input>
   Path/Filename [<home dir>/config.txt]:path to configuration file
   Section (all|chassis|switch [all]): all
   .
   .
   .
   Do you want to continue [y/n]: y
   Password: <user input>
   ```

   After entering your password, the switch downloads and executes the configuration file.

2. Persistently enable the switch:

   `switchcfgpersistentenable`

   The example shows how to persistently enable FC switch_A_1.

   ```
   FC_switch_A_1:admin> switchcfgpersistentenable
   ```

3. Run the following command to confirm that the configuration file has set the switch domain:

   `switchShow`

   Each switch is assigned a different domain number depending on which configuration file the switch used.

   ```
   FC_switch_A_1:admin> switchShow
   switchName: FC_switch_A_1
   switchType: 109.1
   switchState: Online
   switchMode: Native
   switchRole: Subordinate
   switchDomain: 5
   ```

4. Verify that your switch is assigned the correct domain value as indicated in the following table.

Fabric	Switch	Switch domain
1	A_1	5
	B_1	7
2	A_2	6
	B_2	8

5. Change the port speed:

   `portcfgspeed`

   ```
   FC_switch_A_1:admin> portcfgspeed port number port speed
   ```

   By default, all the ports are configured to operate at 16 Gbps. You might change the port speed for the following reasons:

   - The interconnect switch ports speed should be changed when an 8-Gbps FC-VI adapter is used and the switch port speed should set to 8 Gbps.
   - The switch ports speed should be changed when an 8-Gbps HBA adapter is used for ATTO FibreBridge 6500N.
   - The ISL ports' speed must be changed when the ISL is not capable of running at 16 Gbps.

6. Calculate the ISL distance.

   Due to the behavior of the FC-VI, you must set the distance to 1.5 times the real distance with a minimum of 10 (LE). The distance for the ISL is calculated as follows, rounded up to the next full kilometer: 1.5 × real distance = distance.

   If the distance is 3 km, then 1.5 × 3 km = 4.5. This is lower than 10; therefore, you must set the ISL to the LE distance level.

   The distance is 20 km, then 1.5 × 20 km = 30. You must set the ISL to the LS distance level.

7. Set the distance for each ISL port:

   `portcfglongdistance` *`port level vc_link_init`* `-distance` *`distance_value`*

   A vc_link_init value of 1 uses the fillword "ARB" by default. A value of 0 uses the fillword "IDLE". The required value might vary depending on the link you use. In this example, the default is set and the distance is assumed to be 20 km. Hence, the setting is "30" with a vc_link_init value of "1", and the ISL port is "21".

   Example: LS

   ```
   FC_switch_A_1:admin> portcfglongdistance 21 LS 1 -distance 30
   ```

Example: LE

```
FC_switch_A_1:admin> portcfglongdistance 21 LE 1
```

8. Verify if the IP address is set correctly:

   `ipAddrshow`

   ```
   FC_switch_A_1:admin> ipAddrshow
   ```

   You can set the IP address with the following command if required:

   `ipAddrSet`

9. Set the timezone from the switch prompt:

   `tstimezone --interactive`

   You should respond to the prompts as required.

   ```
   FC_switch_A_1:admin>  tstimezone --interactive
   ```

10. Reboot the switch:

    `reboot`

    The example shows how to reboot FC switch _A_1.

    ```
    FC_switch_A_1:admin> reboot
    ```

11. Verify the distance setting:

    `portbuffershow`

    A distance setting of LE appears as 10 km.

```
FC_Switch_A_1:admin> portbuffershow
User Port Lx    Max/Resv Buffer Needed  Link     Remaining
Port Type Mode Buffers  Usage  Buffers Distance Buffers
---- ---- ---- -------- ------ -------- --------- ----------
...
21    E    -      8      67     67      30  km
22    E    -      8      67     67      30  km
...
23    -    8      0       -      -      466
```

12. Reconnect the ISL cables to the ports on the switches where they were removed.

    The ISL cables were disconnected when the factory settings were reset to the default settings.

    Resetting the Brocade FC switch to factory defaults

13. Validate the configuration.

    a. Verify that the switches form one fabric:

       `switchshow`

       The following example shows the output for a configuration that uses ISLs on ports 20 and 21.

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:       5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
===========================================
...
20   20   010C00   id    16G  Online FC   LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream)(trunk master)
21   21   010D00   id    16G  Online FC   LE E-Port  (Trunk port,
master is Port 20)
...
```

    b. Confirm the configuration of the fabrics:

```
fabricshow
```

```
FC_switch_A_1:admin> fabricshow
   Switch ID   Worldwide Name      Enet IP Addr FC IP Addr Name
-----------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"
```

c. Verify that the ISLs are working:

```
islshow
```

```
FC_switch_A_1:admin> islshow
```

d. Confirm that zoning is properly replicated:

```
cfgshow
zoneshow
```

Both outputs should show the same configuration information and zoning information for both switches.

e. If trunking is used, you can confirm the trunking with the following command: **`trunkShow`**

```
FC_switch_A_1:admin> trunkshow
```

Configuring the Cisco FC switches with RCF files

To configure a Cisco FC switch, you must reset the switch settings to factory defaults, install the switch software, and download and apply the reference configuration (RCF) files that provide the complete switch settings for certain configurations.

Resetting the Cisco FC switch to factory defaults

Before installing a new software version and RCFs, you must erase the Cisco switch configuration and perform basic configuration.

About this task

You must repeat these steps on each of the FC switches in the MetroCluster fabric configuration.

> ⓘ The outputs shown are for Cisco IP switches; however, these steps are also applicable for Cisco FC switches.

Steps

1. Reset the switch to factory defaults:

   a. Erase the existing configuration:
      `write erase`

   b. Reload the switch software:
      `reload`

      The system reboots and enters the configuration wizard. During the boot, if you receive the prompt Abort Auto Provisioning and continue with normal setup?(yes/no)[n], you should respond **`yes`** to proceed.

   c. In the configuration wizard, enter the basic switch settings:

      - Admin password
      - Switch name
      - Out-of-band management configuration
      - Default gateway
      - SSH service (Remote Support Agent) After completing the configuration wizard, the switch reboots.

   d. When prompted, enter the user name and password to log in to the switch.

      The following example shows the prompts and system responses when logging in to the switch. The angle brackets (**<<<**) show where you enter the information.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password  **<<<**
  Confirm the password for "admin": password  **<<<**
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

   e. Enter basic information in the next set of prompts, including the switch name, management address, and gateway, and enter **`rsa`** for the SSH key as shown in the example:

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

The final set of prompt completes the configuration:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-
Plane is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Save the configuration:

```
IP_switch_A_1# copy running-config startup-config
```

3. Reboot the switch and wait for the switch to reload:

```
IP_switch_A_1# reload
```

4. Repeat the previous steps on the other three switches in the MetroCluster fabric configuration.

Downloading and installing the Cisco FC switch NX-OS software

You must download the switch operating system file and RCF file to each switch in the MetroCluster fabric configuration.

Before you begin

This task requires file transfer software, such as FTP, TFTP, SFTP, or SCP, to copy the files to the switches.

About this task

These steps must be repeated on each of the FC switches in the MetroCluster fabric configuration.

You must use the supported switch software version.

NetApp Hardware Universe

> The outputs shown are for Cisco IP switches; however, these steps are also applicable for Cisco FC switches.

Steps

1. Download the supported NX-OS software file.

   Cisco download page

2. Copy the switch software to the switch:

   `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

   In this example, the `nxos.7.0.3.I4.6.bin` file is copied from SFTP server 10.10.99.99 to the local bootflash:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                  100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Verify on each switch that the switch NX-OS files are present in each switch's bootflash directory:

   `dir bootflash`

   The following example shows that the files are present on `IP_switch_A_1`:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Install the switch software:

```
install all system bootflash:nxos.version-number.bin kickstart
bootflash:nxos.version-kickstart-number.bin
```

```
IP_switch_A_1#  install all system bootflash:nxos.7.0.3.I4.6.bin
kickstart bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable
"system".
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS
...
```

The switch reboot automatically after the switch software has installed.

5. Wait for the switch to reload and then log in to the switch.

   After the switch has rebooted the login prompt is displayed:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verify that the switch software has been installed:

   `show version`

   The following example shows the output:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Repeat these steps on the remaining three FC switches in the MetroCluster fabric configuration.

Downloading and installing the Cisco FC RCF files

You must download the RCF file to each switch in the MetroCluster fabric configuration.

Before you begin

This task requires file transfer software, such as FTP, Trivial File Transfer Protocol (TFTP), SFTP, or Secure

Copy Protocol (SCP), to copy the files to the switches.

About this task

These steps must be repeated on each of the Cisco FC switches in the MetroCluster fabric configuration.

You must use the supported switch software version.

NetApp Hardware Universe

There are four RCF files, one for each of the four switches in the MetroCluster fabric configuration. You must use the correct RCF files for the switch model you are using.

Switch	RCF file
FC_switch_A_1	`NX3232_v1.80_Switch-A1.txt`
FC_switch_A_2	`NX3232_v1.80_Switch-A2.txt`
FC_switch_B_1	`NX3232_v1.80_Switch-B1.txt`
FC_switch_B_2	`NX3232_v1.80_Switch-B2.txt`

> The outputs shown are for Cisco IP switches; however, these steps are also applicable for Cisco FC switches.

Steps

1. Download the Cisco FC RCF files from the MetroCluster RCF download page.
2. Copy the RCF files to the switches.
   a. Copy the RCF files to the first switch:

      ```
      copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
      bootflash: vrf management
      ```

      In this example, the `NX3232_v1.80_Switch-A1.txt` RCF file is copied from the SFTP server at `10.10.99.99` to the local bootflash. You must use the IP address of your TFTP/SFTP server and the file name of the RCF file that you need to install.

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/NX3232_v1.8T-
X1_Switch-A1.txt bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

b. Repeat the previous substep for each of the other three switches, being sure to copy the matching RCF file to the corresponding switch.

3. Verify on each switch that the RCF file is present in each switch's `bootflash` directory:

   `dir bootflash:`

   The following example shows that the files are present on IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
       5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Copy the matching RCF file from the local bootflash to the running configuration on each switch:

   `copy bootflash:`*`switch-specific-RCF`*`.txt running-config`

5. Copy the RCF files from the running configuration to the startup configuration on each switch:

   `copy running-config startup-config`

You should see output similar to the following:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch_A_1# copy running-config startup-config
```

6. Reload the switch:

   `reload`

```
IP_switch_A_1# reload
```

7. Repeat the previous steps on the other three switches in the MetroCluster IP configuration.

Configuring the Brocade FC switches manually

You must configure each of the Brocade switch fabrics in the MetroCluster configuration.

Before you begin

- You must have a PC or UNIX workstation with Telnet or Secure Shell (SSH) access to the FC switches.
- You must be using four supported Brocade switches of the same model with the same Brocade Fabric Operating System (FOS) version and licensing.

  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.
- The four supported Brocade switches must be connected to two fabrics of two switches each, with each fabric spanning both sites.
- Each storage controller must have four initiator ports available to connect to the switch fabrics. Two initiator ports must be connected from each storage controller to each fabric.

  > You can configure FAS8020, AFF8020, FAS8200, and AFF A300 systems with two initiators ports per controller (a single initiator port to each fabric) if all the following criteria are met:

  - There are fewer than four FC initiator ports available to connect the disk storage and no additional ports can be configured as FC initiators.
  - All slots are in use and no FC initiator card can be added.

About this task

- You should enable Inter-Switch Link (ISL) trunking when it is supported by the links.

  Considerations for using TDM/WDM equipment with fabric-attached MetroCluster configurations
- All ISLs must have the same length and same speed in one fabric.

  Different lengths can be used in the different fabrics. The same speed must be used in all fabrics.

- Metro-E and TDM (SONET/SDH) are not supported, and any non-FC native framing or signaling is not supported.

  Metro-E means Ethernet framing or signaling occurs either natively over a Metro distance or through some time-division multiplexing (TDM), multiprotocol label switching (MPLS), or wavelength-division multiplexing (WDM).

- TDMs, FCR (native FC Routing), or FCIP extensions are not supported for the MetroCluster FC switch fabric.
- Certain switches in the MetroCluster FC switch fabric support encryption or compression, and sometimes support both.

  NetApp Interoperability Matrix Tool (IMT)

  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.

- The Brocade Virtual Fabric (VF) feature is not supported.
- FC zoning based on domain port is supported, but zoning based on worldwide name (WWN) is not supported.

Reviewing Brocade license requirements

You need certain licenses for the switches in a MetroCluster configuration. You must install these licenses on all four switches.

About this task

The MetroCluster configuration has the following Brocade license requirements:

- Trunking license for systems using more than one ISL, as recommended.
- Extended Fabric license (for ISL distances over 6 km)
- Enterprise license for sites with more than one ISL and an ISL distance greater than 6 km

  The Enterprise license includes Brocade Network Advisor and all licenses except for additional port licenses.

Step

1. Verify that the licenses are installed:

   ```
   licenseshow
   ```

   If you do not have these licenses, you should contact your sales representative before proceeding.

Setting the Brocade FC switch values to factory defaults

You must set the switch to its factory defaults to ensure a successful configuration. You must also assign each switch a unique name.

About this task

In the examples in this procedure, the fabric consists of BrocadeSwitchA and BrocadeSwitchB.

Steps

1. Make a console connection and log in to both switches in one fabric.
2. Disable the switch persistently:

   `switchcfgpersistentdisable`

   This ensures the switch will remain disabled after a reboot or fastboot. If this command is not available, use the `switchdisable` command.

   The following example shows the command on BrocadeSwitchA:

   ```
   BrocadeSwitchA:admin> switchcfgpersistentdisable
   ```

   The following example shows the command on BrocadeSwitchB:

   ```
   BrocadeSwitchA:admin> switchcfgpersistentdisable
   ```

3. Set the switch name:

   `switchname switch_name`

   The switches should each have a unique name. After setting the name, the prompt changes accordingly.

   The following example shows the command on BrocadeSwitchA:

   ```
   BrocadeSwitchA:admin> switchname "FC_switch_A_1"
   FC_switch_A_1:admin>
   ```

   The following example shows the command on BrocadeSwitchB:

   ```
   BrocadeSwitchB:admin> switchname "FC_Switch_B_1"
   FC_switch_B_1:admin>
   ```

4. Set all ports to their default values:

   `portcfgdefault`

   This must be done for all ports on the switch.

   The following example shows the commands on FC_switch_A_1:

```
FC_switch_A_1:admin> portcfgdefault 0
FC_switch_A_1:admin> portcfgdefault 1
...
FC_switch_A_1:admin> portcfgdefault 39
```

The following example shows the commands on FC_switch_B_1:

```
FC_switch_B_1:admin> portcfgdefault 0
FC_switch_B_1:admin> portcfgdefault 1
...
FC_switch_B_1:admin> portcfgdefault 39
```

5. Clear the zoning information:

   `cfgdisable`

   `cfgclear`

   `cfgsave`

   The following example shows the commands on FC_switch_A_1:

```
FC_switch_A_1:admin> cfgdisable
FC_switch_A_1:admin> cfgclear
FC_switch_A_1:admin> cfgsave
```

   The following example shows the commands on FC_switch_B_1:

```
FC_switch_B_1:admin> cfgdisable
FC_switch_B_1:admin> cfgclear
FC_switch_B_1:admin> cfgsave
```

6. Set the general switch settings to default:

   `configdefault`

   The following example shows the command on FC_switch_A_1:

```
FC_switch_A_1:admin> configdefault
```

   The following example shows the command on FC_switch_B_1:

```
FC_switch_B_1:admin> configdefault
```

7. Set all ports to non-trunking mode:

   `switchcfgtrunk 0`

   The following example shows the command on FC_switch_A_1:

   ```
   FC_switch_A_1:admin> switchcfgtrunk 0
   ```

   The following example shows the command on FC_switch_B_1:

   ```
   FC_switch_B_1:admin> switchcfgtrunk 0
   ```

8. On Brocade 6510 switches, disable the Brocade Virtual Fabrics (VF) feature:

   `fosconfig options`

   The following example shows the command on FC_switch_A_1:

   ```
   FC_switch_A_1:admin> fosconfig --disable vf
   ```

   The following example shows the command on FC_switch_B_1:

   ```
   FC_switch_B_1:admin> fosconfig --disable vf
   ```

9. Clear the Administrative Domain (AD) configuration:

   `ad options`

   The following example shows the commands on FC_switch_A_1:

   ```
   FC_switch_A_1:admin> switch:admin> ad --select AD0
   FC_switch_A_1:> defzone --noaccess
   FC_switch_A_1:> cfgsave
   FC_switch_A_1:> exit
   FC_switch_A_1:admin> ad --clear -f
   FC_switch_A_1:admin> ad --apply
   FC_switch_A_1:admin> ad --save
   FC_switch_A_1:admin> exit
   ```

   The following example shows the commands on FC_switch_B_1:

```
FC_switch_B_1:admin> switch:admin> ad --select AD0
FC_switch_A_1:> defzone --noaccess
FC_switch_A_1:> cfgsave
FC_switch_A_1:> exit
FC_switch_B_1:admin> ad --clear -f
FC_switch_B_1:admin> ad --apply
FC_switch_B_1:admin> ad --save
FC_switch_B_1:admin> exit
```

10. Reboot the switch:

    `reboot`

    The following example shows the command on FC_switch_A_1:

    ```
    FC_switch_A_1:admin> reboot
    ```

    The following example shows the command on FC_switch_B_1:

    ```
    FC_switch_B_1:admin> reboot
    ```

Configuring basic switch settings

You must configure basic global settings, including the domain ID, for Brocade switches.

About this task

This task contains steps that must be performed on each switch at both of the MetroCluster sites.

In this procedure, you set the unique domain ID for each switch as shown in the following example. In the example, domain IDs 5 and 7 form fabric_1, and domain IDs 6 and 8 form fabric_2.

- FC_switch_A_1 is assigned to domain ID 5
- FC_switch_A_2 is assigned to domain ID 6
- FC_switch_B_1 is assigned to domain ID 7
- FC_switch_B_2 is assigned to domain ID 8

Steps

1. Enter configuration mode:

   `configure`

2. Proceed through the prompts:

   a. Set the domain ID for the switch.

   b. Press **Enter** in response to the prompts until you get to "RDP Polling Cycle", and then set that value to `0` to disable the polling.

c. Press **Enter** until you return to the switch prompt.

```
FC_switch_A_1:admin> configure
Fabric parameters = y
Domain_id = 5
.
.

RSCN Transmission Mode [yes, y, no, no: [no] y

End-device RSCN Transmission Mode
 (0 = RSCN with single PID, 1 = RSCN with multiple PIDs, 2 = Fabric
RSCN): (0..2) [1]
Domain RSCN To End-device for switch IP address or name change
 (0 = disabled, 1 = enabled): (0..1) [0] 1

.
.
RDP Polling Cycle(hours)[0 = Disable Polling]: (0..24) [1] 0
```

3. If you are using two or more ISLs per fabric, then you can configure either in-order delivery (IOD) of frames or out-of-order (OOD) delivery of frames.

> The standard IOD settings are recommended. You should configure OOD only if necessary.

Considerations for using TDM/WDM equipment with fabric-attached MetroCluster configurations

a. The following steps must be performed on each switch fabric to configure IOD of frames:

i. Enable IOD:

```
iodset
```

ii. Set the Advanced Performance Tuning (APT) policy to 1:

```
aptpolicy 1
```

iii. Disable Dynamic Load Sharing (DLS):

```
dlsreset
```

iv. Verify the IOD settings by using the `iodshow`, `aptpolicy`, and `dlsshow` commands.

For example, issue the following commands on FC_switch_A_1:

```
FC_switch_A_1:admin> iodshow
    IOD is set

    FC_switch_A_1:admin> aptpolicy
    Current Policy: 1 0(ap)

    3 0(ap) : Default Policy
    1: Port Based Routing Policy
    3: Exchange Based Routing Policy
         0: AP Shared Link Policy
         1: AP Dedicated Link Policy
    command aptpolicy completed

    FC_switch_A_1:admin> dlsshow
    DLS is not set
```

v. Repeat these steps on the second switch fabric.

b. The following steps must be performed on each switch fabric to configure OOD of frames:

i. Enable OOD:

```
iodreset
```

ii. Set the Advanced Performance Tuning (APT) policy to 3:

```
aptpolicy 3
```

iii. Disable Dynamic Load Sharing (DLS):

```
dlsreset
```

iv. Verify the OOD settings:

```
iodshow
```

```
aptpolicy
```

```
dlsshow
```

For example, issue the following commands on FC_switch_A_1:

```
FC_switch_A_1:admin> iodshow
    IOD is not set

    FC_switch_A_1:admin> aptpolicy
    Current Policy: 3 0(ap)
    3 0(ap) : Default Policy
    1: Port Based Routing Policy
    3: Exchange Based Routing Policy
    0: AP Shared Link Policy
    1: AP Dedicated Link Policy
    command aptpolicy completed


    FC_switch_A_1:admin> dlsshow
    DLS is set by default with current routing policy
```

v. Repeat these steps on the second switch fabric.

> When configuring ONTAP on the controller modules, OOD must be explicitly configured on each controller module in the MetroCluster configuration.

Configuring in-order delivery or out-of-order delivery of frames on ONTAP software

4. Verify that the switch is using the dynamic port licensing method.
   a. Run the license command:

      `licensePort --show`

```
FC_switch_A_1:admin> licenseport -show
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

> Brocade FabricOS versions before 8.0 run the following commands as admin and versions 8.0 and later run them as root.

   b. Enable the root user.

      If the root user is already disabled by Brocade, enable the root user as shown in the following example:

```
FC_switch_A_1:admin> userconfig --change root -e yes
FC_switch_A_1:admin> rootaccess --set consoleonly
```

   c. Run the license command:

licensePort --show

```
FC_switch_A_1:root> licenseport -show
24 ports are available in this switch
Full POD license is installed
Dynamic POD method is in use
```

d. Change the license method to dynamic:

`licenseport --method dynamic`

> If the dynamic license method is not in use (if the method is static), you must change the license method to dynamic. Skip this step if the dynamic license method is in use.

```
FC_switch_A_1:admin> licenseport --method dynamic
The POD method has been changed to dynamic.
Please reboot the switch now for this change to take effect
```

5. Enable the trap for T11-FC-ZONE-SERVER-MIB to provide successful health monitoring of the switches in ONTAP:

   a. Enable the T11-FC-ZONE-SERVER-MIB:

   `snmpconfig --set mibCapability -mib_name T11-FC-ZONE-SERVER-MIB -bitmask 0x3f`

   b. Enable the T11-FC-ZONE-SERVER-MIB trap:

   `snmpconfig --enable mibcapability -mib_name SW-MIB -trap_name swZoneConfigChangeTrap`

   c. Repeat the previous steps on the second switch fabric.

6. **Optional**: If you set the community string to a value other than "public", you must configure the ONTAP Health Monitors using the community string you specify:

   a. Change the existing community string:

   `snmpconfig --set snmpv1`

   b. Press **Enter** until you see "Community (ro): [public]" text.

   c. Enter the desired community string.

   On FC_switch_A_1:

```
FC_switch_A_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm     <<<<<< change the community string
to the desired value,
Trap Recipient's IP address : [0.0.0.0]    in this example it is set
to "mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_A_1:admin>
```

On FC_switch_B_1:

```
FC_switch_B_1:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [public] mcchm      <<<<<< change the community
string to the desired value,
Trap Recipient's IP address : [0.0.0.0]     in this example it is set
to "mcchm"
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [0.0.0.0]
Committing configuration.....done.
FC_switch_B_1:admin>
```

7. Reboot the switch:

   `reboot`

   On FC_switch_A_1:

```
FC_switch_A_1:admin> reboot
```

On FC_switch_B_1:

```
FC_switch_B_1:admin> reboot
```

8. Persistently enable the switch:

   `switchcfgpersistentenable`

   On FC_switch_A_1:

```
FC_switch_A_1:admin> switchcfgpersistentenable
```

   On FC_switch_B_1:

```
FC_switch_B_1:admin> switchcfgpersistentenable
```

Configuring basic switch settings on a Brocade DCX 8510-8 switch

You must configure basic global settings, including the domain ID, for Brocade switches.

About this task

You must perform the steps on each switch at both MetroCluster sites. In this procedure, you set the domain ID for each switch as shown in the following examples:

- FC_switch_A_1 is assigned to domain ID 5
- FC_switch_A_2 is assigned to domain ID 6
- FC_switch_B_1 is assigned to domain ID 7
- FC_switch_B_2 is assigned to domain ID 8

In the previous example, domain IDs 5 and 7 form fabric_1, and domain IDs 6 and 8 form fabric_2.

> You can also use this procedure to configure the switches when you are only using one DCX 8510-8 switch per site.

Using this procedure, you should create two logical switches on each Brocade DCX 8510-8 switch. The two logical switches created on both Brocade DCX8510-8 switches will form two logical fabrics as shown in the following examples:

- LOGICAL FABRIC 1: Switch1/Blade1 and Switch 2 Blade 1
- LOGICAL FABRIC 2: Switch1/Blade2 and Switch 2 Blade 2

Steps

1. Enter the command mode:

   `configure`

2. Proceed through the prompts:

   a. Set the domain ID for the switch.

   b. Keep selecting **Enter** until you get to "RDP Polling Cycle", and then set the value to `0` to disable the polling.

   c. Select **Enter** until you return to the switch prompt.

   ```
   FC_switch_A_1:admin> configure
   Fabric parameters = y
   Domain_id = `5


   RDP Polling Cycle(hours)[0 = Disable Polling]: (0..24) [1] 0
   `
   ```

3. Repeat these steps on all switches in fabric_1 and fabric_2.

4. Configure the virtual fabrics.

   a. Enable virtual fabrics on the switch:

      `fosconfig --enablevf`

   b. Configure the system to use the same base configuration on all logical switches:

      `configurechassis`

      The following example shows the output for the `configurechassis` command:

      ```
      System (yes, y, no, n): [no] n
      cfgload attributes (yes, y, no, n): [no] n
      Custom attributes (yes, y, no, n): [no] y
      Config Index (0 to ignore): (0..1000) [3]:
      ```

5. Create and configure the logical switch:

   `scfg --create fabricID`

6. Add all ports from a blade to the virtual fabric:

   `lscfg --config fabricID -slot slot -port lowest-port - highest-port`

   > The blades forming a logical fabric (e.g. Switch 1 Blade 1 and Switch 3 Blade 1) need to have the same fabric ID.

```
setcontext fabricid
switchdisable
configure
<configure the switch per the above settings>
switchname unique switch name
switchenable
```

Related information

Requirements for using a Brocade DCX 8510-8 switch

Configuring E-ports on Brocade FC switches using FC ports

For Brocade switches on which the Inter-Switch Links (ISL) are configured using FC ports, you must configure the switch ports on each switch fabric that connect the ISL. These ISL ports are also known as E-ports.

Before you begin

- All of the ISLs in an FC switch fabric must be configured with the same speed and distance.
- The combination of the switch port and small form-factor pluggable (SFP) must support the speed.
- The supported ISL distance depends on the FC switch model.

  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.

- The ISL link must have a dedicated lambda, and the link must be supported by Brocade for the distance, switch type, and Fabric Operating System (FOS).

About this task

You must not use the L0 setting when issuing the `portCfgLongDistance` command. Instead, you should use the LE or LS setting to configure the distance on the Brocade switches with a minimum of LE distance level.

You must not use the LD setting when issuing the `portCfgLongDistance` command when working with xWDM/TDM equipment. Instead, you should use the LE or LS setting to configure the distance on the Brocade switches.

You must perform this task for each FC switch fabric.

The following tables show the ISL ports for different switches and different number of ISLs in a configuration running ONTAP 9.1 or 9.2. The examples shown in this section are for a Brocade 6505 switch. You should modify the examples to use ports that apply to your switch type.

If your configuration is running ONTAP 9.0 or earlier, see the Port assignments for FC switches when using ONTAP 9.0 section in the *Fabric-attached MetroCluster Installation and Configuration Guide*.

You must use the required number of ISLs for your configuration.

Switch model	ISL port	Switch port

Brocade 6520	ISL port 1	23
	ISL port 2	47
	ISL port 3	71
	ISL port 4	95
Brocade 6505	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23
Brocade 6510 and Brocade DCX 8510-8	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47
Brocade 7810	ISL port 1	ge2 (10-Gbps)
	ISL port 2	ge3(10-Gbps)
	ISL port 3	ge4 (10-Gbps)
	ISL port 4	ge5 (10-Gbps)
	ISL port 5	ge6 (10-Gbps)
	ISL port 6	ge7 (10-Gbps)
Brocade 7840 **Note:** The Brocade 7840 switch supports either two 40 Gbps VE-ports or up to four 10 Gbps VE-ports per switch for the creation of FCIP ISLs.	ISL port 1	ge0 (40-Gbps) or ge2 (10-Gbps)
	ISL port 2	ge1 (40-Gbps) or ge3 (10-Gbps)
	ISL port 3	ge10 (10-Gbps)
	ISL port 4	ge11 (10-Gbps)

Brocade G610	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23
Brocade G620, G620-1, G630, G630-1, G720	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46

Steps

1. Configure the port speed:

   `portcfgspeed port-numberspeed`

   You must use the highest common speed that is supported by the components in the path.

   In the following example, there are two ISLs for each fabric:

```
FC_switch_A_1:admin> portcfgspeed 20 16
FC_switch_A_1:admin> portcfgspeed 21 16

FC_switch_B_1:admin> portcfgspeed 20 16
FC_switch_B_1:admin> portcfgspeed 21 16
```

2. Configure the trunking mode for each ISL:

   `portcfgtrunkport port-number`

   - If you are configuring the ISLs for trunking (IOD), set the portcfgtrunk port-numberport-number to 1 as shown in the following example:

```
FC_switch_A_1:admin> portcfgtrunkport 20 1
FC_switch_A_1:admin> portcfgtrunkport 21 1
FC_switch_B_1:admin> portcfgtrunkport 20 1
FC_switch_B_1:admin> portcfgtrunkport 21 1
```

- If you do not want to configure the ISL for trunking (OOD), set portcfgtrunkport-number to 0 as shown in the following example:

```
FC_switch_A_1:admin> portcfgtrunkport 20 0
FC_switch_A_1:admin> portcfgtrunkport 21 0
FC_switch_B_1:admin> portcfgtrunkport 20 0
FC_switch_B_1:admin> portcfgtrunkport 21 0
```

3. Enable QoS traffic for each of the ISL ports:

   `portcfgqos --enable port-number`

   In the following example, there are two ISLs per switch fabric:

```
FC_switch_A_1:admin> portcfgqos --enable 20
FC_switch_A_1:admin> portcfgqos --enable 21

FC_switch_B_1:admin> portcfgqos --enable 20
FC_switch_B_1:admin> portcfgqos --enable 21
```

4. Verify the settings:

   `portCfgShow command`

   The following example shows the output for a configuration that uses two ISLs cabled to port 20 and port 21. The Trunk Port setting should be ON for IOD and OFF for OOD:

```
Ports of Slot 0   12  13   14 15    16  17  18  19   20  21 22  23    24
25  26  27
----------------+---+---+---+-----+---+---+---+----+---+---+----+
-----+---+---+---
Speed             AN  AN  AN  AN    AN  AN  8G  AN   AN  AN  16G  16G
AN  AN  AN  AN
Fill Word         0   0   0   0     0   0   3   0    0   0   3   3     3
0   0   0
AL_PA Offset 13   ..  ..  ..  ..    ..  ..  ..  ..   ..  ..  ..  ..
..  ..  ..  ..
Trunk Port        ..  ..  ..  ..    ..  ..  ..  ..   ON  ON  ..  ..
..  ..  ..  ..
```

```
Long Distance      ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
VC Link Init       ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
Locked L_Port      ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
Locked G_Port      ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
Disabled E_Port    ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
Locked E_Port      ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
ISL R_RDY Mode     ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
RSCN Suppressed    ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
Persistent Disable..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
LOS TOV enable     ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
NPIV capability    ON  ON  ON  ON    ON  ON  ON  ON    ON  ON  ON  ON
ON  ON  ON  ON
NPIV PP Limit     126 126 126 126   126 126 126 126  126 126 126 126
126 126 126 126
QOS E_Port         AE  AE  AE  AE    AE  AE  AE  AE    AE  AE  AE  AE
AE  AE  AE  AE
Mirror Port        ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
Rate Limit         ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
Credit Recovery    ON  ON  ON  ON    ON  ON  ON  ON    ON  ON  ON  ON
ON  ON  ON  ON
Fport Buffers      ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
Port Auto Disable ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..
CSCTL mode         ..  ..  ..  ..    ..  ..  ..  ..    ..  ..  ..  ..
..  ..  ..  ..

Fault Delay       0  0  0  0    0  0  0  0    0  0  0  0    0  0  0  0
```

5. Calculate the ISL distance.

   Because of the behavior of FC-VI, the distance must be set to 1.5 times the real distance with a minimum distance of 10 km (using the LE distance level).

   The distance for the ISL is calculated as follows, rounded up to the next full kilometer:

1.5 × real_distance = distance

If the distance is 3 km, then 1.5 × 3 km = 4.5 km. This is lower than 10 km, so the ISL must be set to the LE distance level.

If the distance is 20 km, then 1.5 × 20 km = 30 km. The ISL must be set to 30 km and must use the LS distance level.

6. Set the distance on each ISL port:

   `portcfglongdistance` *`portdistance-level`* `vc_link_init` *`distance`*

   A `vc_link_init` value of `1` uses the ARB fill word (default). A value of `0` uses IDLE. The required value might depend on the link being used. The commands must be repeated for each ISL port.

   For an ISL distance of 3 km, as given in the example in the previous step, the setting is 4.5 km with the default `vc_link_init` value of `1`. Because a setting of 4.5 km is lower than 10 km, the port needs to be set to the LE distance level:

   ```
   FC_switch_A_1:admin> portcfglongdistance 20 LE 1

   FC_switch_B_1:admin> portcfglongdistance 20 LE 1
   ```

   For an ISL distance of 20 km, as given in the example in the previous step, the setting is 30 km with the default vc_link_init value of `1`:

   ```
   FC_switch_A_1:admin> portcfglongdistance 20 LS 1 -distance 30

   FC_switch_B_1:admin> portcfglongdistance 20 LS 1 -distance 30
   ```

7. Verify the distance setting:

   `portbuffershow`

   A distance level of LE appears as 10 km.

   The following example shows the output for a configuration that uses ISLs on port 20 and port 21:

```
FC_switch_A_1:admin> portbuffershow

User  Port     Lx      Max/Resv    Buffer Needed    Link      Remaining
Port  Type    Mode     Buffers     Usage  Buffers   Distance  Buffers
----  ----    ----     -------     ------ -------   --------- ---------
...
 20     E      -          8          67      67       30km
 21     E      -          8          67      67       30km
...
 23            -          8           0      -        -        466
```

8. Verify that both switches form one fabric:

   `switchshow`

   The following example shows the output for a configuration that uses ISLs on port 20 and port 21:

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Subordinate
switchDomain:       5
switchId:   fffc01
switchWwn:  10:00:00:05:33:86:89:cb
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
===========================================
...
20   20  010C00   id    16G  Online FC  LE E-Port
10:00:00:05:33:8c:2e:9a "FC_switch_B_1" (downstream)(trunk master)
21   21  010D00   id    16G  Online FC  LE E-Port  (Trunk port, master
is Port 20)
...

FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 109.1
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       7
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State Proto
==============================================
...
20   20  030C00   id    16G  Online  FC  LE E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)(Trunk master)
21   21  030D00   id    16G  Online  FC  LE E-Port  (Trunk port, master
is Port 20)
...
```

9. Confirm the configuration of the fabrics:

```
fabricshow
```

```
FC_switch_A_1:admin> fabricshow
   Switch ID   Worldwide Name      Enet IP Addr FC IP Addr Name
-----------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"
3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1"
```

```
FC_switch_B_1:admin> fabricshow
   Switch ID   Worldwide Name     Enet IP Addr FC IP Addr   Name
----------------------------------------------------------------
1: fffc01 10:00:00:05:33:86:89:cb 10.10.10.55  0.0.0.0
"FC_switch_A_1"

3: fffc03 10:00:00:05:33:8c:2e:9a 10.10.10.65  0.0.0.0
>"FC_switch_B_1
```

10. Confirm the trunking of the ISLs:

```
trunkshow
```

- If you are configuring the ISLs for trunking (IOD), you should see output similar to the following:

```
FC_switch_A_1:admin> trunkshow
 1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
    21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16
 FC_switch_B_1:admin> trunkshow
 1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
    21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16
```

- If you are not configuring the ISLs for trunking (OOD), you should see output similar to the following:

```
FC_switch_A_1:admin> trunkshow
 1: 20-> 20 10:00:00:05:33:ac:2b:13 3 deskew 15 MASTER
 2: 21-> 21 10:00:00:05:33:8c:2e:9a 3 deskew 16 MASTER
FC_switch_B_1:admin> trunkshow
 1: 20-> 20 10:00:00:05:33:86:89:cb 3 deskew 15 MASTER
 2: 21-> 21 10:00:00:05:33:86:89:cb 3 deskew 16 MASTER
```

11. Repeat Step 1 through Step 10 for the second FC switch fabric.

Related information

Port assignments for FC switches when using ONTAP 9.1 and later

Configuring 10 Gbps VE ports on Brocade FC 7840 switches

When using the 10 Gbps VE ports (which use FCIP) for ISLs, you must create IP interfaces on each port, and configure FCIP tunnels and circuits in each tunnel.

About this task

This procedure must be performed on each switch fabric in the MetroCluster configuration.

The examples in this procedure assume that the two Brocade 7840 switches have the following IP addresses:

- FC_switch_A_1 is local.
- FC_switch_B_1 is remote.

Steps

1. Create IP interface (ipif) addresses for the 10 Gbps ports on both switches in the fabric:

   `portcfg ipif FC_switch1_namefirst_port_name create FC_switch1_IP_address netmask netmask_number vlan 2 mtu auto`

   The following command creates ipif addresses on ports ge2.dp0 and ge3.dp0 of FC_switch_A_1:

   ```
   portcfg ipif  ge2.dp0 create  10.10.20.71 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge3.dp0 create  10.10.21.71 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

   The following command creates ipif addresses on ports ge2.dp0 and ge3.dp0 of FC_switch_B_1:

   ```
   portcfg ipif  ge2.dp0 create  10.10.20.72 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge3.dp0 create  10.10.21.72 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

2. Verify that the ipif addresses were created successfully on both switches:

   `portshow ipif all`

   The following command shows the ipif addresses on switch FC_switch_A_1:

```
FC_switch_A_1:root> portshow ipif all

 Port         IP Address                     / Pfx  MTU   VLAN  Flags
----------------------------------------------------------------------
--------
 ge2.dp0      10.10.20.71                    / 24   AUTO  2     U R M I
 ge3.dp0      10.10.21.71                    / 20   AUTO  2     U R M I
----------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

The following command shows the ipif addresses on switch FC_switch_B_1:

```
FC_switch_B_1:root> portshow ipif all

 Port         IP Address                     / Pfx  MTU   VLAN  Flags
----------------------------------------------------------------------
--------
 ge2.dp0      10.10.20.72                    / 24   AUTO  2     U R M I
 ge3.dp0      10.10.21.72                    / 20   AUTO  2     U R M I
----------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

3. Create the first of the two FCIP tunnels using the ports on dp0:

   `portcfg fciptunnel`

   This command creates a tunnel with a single circuit.

   The following command creates the tunnel on switch FC_switch_A_1:

```
portcfg fciptunnel 24 create -S 10.10.20.71  -D 10.10.20.72 -b 10000000
-B 10000000
```

   The following command creates the tunnel on switch FC_switch_B_1:

```
portcfg fciptunnel 24 create -S 10.10.20.72  -D 10.10.20.71 -b 10000000
-B 10000000
```

4. Verify that the FCIP tunnels were successfully created:

   `portshow fciptunnel all`

   The following example shows that the tunnels were created and the circuits are up:

```
FC_switch_B_1:root>

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
--------------------------------------------------------------------------------
--------
 24    -         Up      ---------     2d8m    0.05    0.41   3      -
-
--------------------------------------------------------------------------------
--------
 Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON
r=ReservedBW
                 a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
                 I=IP-Ext
```

5. Create an additional circuit for dp0.

   The following command creates a circuit on switch FC_switch_A_1 for dp0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.71 -D 10.10.21.72  --min
-comm-rate 5000000 --max-comm-rate 5000000
```

   The following command creates a circuit on switch FC_switch_B_1 for dp0:

```
portcfg fcipcircuit 24 create 1 -S 10.10.21.72 -D 10.10.21.71  --min
-comm-rate 5000000 --max-comm-rate 5000000
```

6. Verify that all circuits were successfully created:

   `portshow fcipcircuit all`

   The following command shows the circuits and their status:

```
FC_switch_A_1:root> portshow fcipcircuit all

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
--------------------------------------------------------------------------
--------
 24    0 ge2     Up      ---va---4    2d12m    0.02    0.03   3
10000/10000 0/-
 24    1 ge3     Up      ---va---4    2d12m    0.02    0.04   3
10000/10000 0/-
--------------------------------------------------------------------------
--------
 Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
6=IPv6
                 ARL a=Auto r=Reset s=StepDown t=TimedStepDown  S=SLA
```

Configuring 40 Gbps VE-ports on Brocade 7810 and 7840 FC switches

When using the two 40 GbE VE-ports (which use FCIP) for ISLs, you must create IP interfaces on each port, and configure FCIP tunnels and circuits in each tunnel.

About this task

This procedure must be performed on each switch fabric in the MetroCluster configuration.

The examples in this procedure use two switches:

- FC_switch_A_1 is local.
- FC_switch_B_1 is remote.

Steps

1. Create IP interface (ipif) addresses for the 40 Gbps ports on both switches in the fabric:

   `portcfg ipif FC_switch_namefirst_port_name create FC_switch_IP_address netmask netmask_number vlan 2 mtu auto`

   The following command creates ipif addresses on ports ge0.dp0 and ge1.dp0 of FC_switch_A_1:

   ```
   portcfg ipif  ge0.dp0 create  10.10.82.10 netmask 255.255.0.0 vlan 2 mtu
   auto
   portcfg ipif  ge1.dp0 create  10.10.82.11 netmask 255.255.0.0 vlan 2 mtu
   auto
   ```

   The following command creates ipif addresses on ports ge0.dp0 and ge1.dp0 of FC_switch_B_1:

```
portcfg ipif  ge0.dp0 create  10.10.83.10 netmask 255.255.0.0 vlan 2 mtu
auto
portcfg ipif  ge1.dp0 create  10.10.83.11 netmask 255.255.0.0 vlan 2 mtu
auto
```

2. Verify that the ipif addresses were successfully created on both switches:

   `portshow ipif all`

   The following example shows the IP interfaces on FC_switch_A_1:

```
Port         IP Address                     / Pfx  MTU   VLAN  Flags
------------------------------------------------------------------------
---
-----
 ge0.dp0      10.10.82.10                     / 16   AUTO  2     U R M
 ge1.dp0      10.10.82.11                     / 16   AUTO  2     U R M
------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

   The following example shows the IP interfaces on FC_switch_B_1:

```
Port         IP Address                     / Pfx  MTU   VLAN  Flags
------------------------------------------------------------------------
--------
 ge0.dp0      10.10.83.10                     / 16   AUTO  2     U R M
 ge1.dp0      10.10.83.11                     / 16   AUTO  2     U R M
------------------------------------------------------------------------
--------
Flags: U=Up B=Broadcast D=Debug L=Loopback P=Point2Point R=Running
I=InUse
       N=NoArp PR=Promisc M=Multicast S=StaticArp LU=LinkUp X=Crossport
```

3. Create the FCIP tunnel on both switches:

   `portcfig fciptunnel`

   The following command creates the tunnel on FC_switch_A_1:

```
portcfg fciptunnel 24 create -S 10.10.82.10  -D 10.10.83.10 -b 10000000
-B 10000000
```

The following command creates the tunnel on FC_switch_B_1:

```
portcfg fciptunnel 24 create -S 10.10.83.10  -D 10.10.82.10 -b 10000000
-B 10000000
```

4. Verify that the FCIP tunnel has been successfully created:

   `portshow fciptunnel all`

   The following example shows that the tunnel was created and the circuits are up:

```
FC_switch_A_1:root>

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
------------------------------------------------------------------------
--------
 24    -         Up      ---------     2d8m    0.05    0.41   3      -
-
 -----------------------------------------------------------------------
---------
 Flags (tunnel): i=IPSec f=Fastwrite T=TapePipelining F=FICON
r=ReservedBW
                 a=FastDeflate d=Deflate D=AggrDeflate P=Protocol
                 I=IP-Ext
```

5. Create an additional circuit on each switch:

   `portcfg fcipcircuit 24 create 1 -S source-IP-address -D destination-IP-address --min-comm-rate 10000000 --max-comm-rate 10000000`

   The following command creates a circuit on switch FC_switch_A_1 for dp0:

```
portcfg fcipcircuit 24  create 1 -S 10.10.82.11 -D 10.10.83.11  --min
-comm-rate 10000000 --max-comm-rate 10000000
```

The following command creates a circuit on switch FC_switch_B_1 for dp1:

```
portcfg fcipcircuit 24 create 1  -S 10.10.83.11 -D 10.10.82.11  --min
-comm-rate 10000000 --max-comm-rate 10000000
```

6. Verify that all circuits were successfully created:

   `portshow fcipcircuit all`

   The following example lists the circuits and shows that their OpStatus is up:

```
FC_switch_A_1:root> portshow fcipcircuit all

 Tunnel Circuit  OpStatus  Flags    Uptime  TxMBps  RxMBps ConnCnt
CommRt Met/G
--------------------------------------------------------------------------------
 24    0 ge0     Up      ---va---4    2d12m    0.02    0.03   3
10000/10000 0/-
 24    1 ge1     Up      ---va---4    2d12m    0.02    0.04   3
10000/10000 0/-
 --------------------------------------------------------------------------------
 Flags (circuit): h=HA-Configured v=VLAN-Tagged p=PMTU i=IPSec 4=IPv4
6=IPv6
                 ARL a=Auto r=Reset s=StepDown t=TimedStepDown  S=SLA
```

Configuring the non-E-ports on the Brocade switch

You must configure the non-E-ports on the FC switch. In a MetroCluster configuration, these are the ports that connect the switch to the HBA initiators, FC-VI interconnects, and FC-to-SAS bridges. These steps must be done for each port.

About this task

In the following example, the ports connect an FC-to-SAS bridge:

- Port 6 on FC_FC_switch_A_1 at Site_A
- Port 6 on FC_FC_switch_B_1 at Site_B

Steps

1. Configure the port speed for each non-E-port:

   `portcfgspeed portspeed`

   You should use the highest common speed, which is the highest speed supported by all components in the data path: the SFP, the switch port that the SFP is installed on, and the connected device (HBA, bridge, and so on).

   For example, the components might have the following supported speeds:

- The SFP is capable of 4, 8, or 16 GB.
- The switch port is capable of 4, 8, or 16 GB.
- The connected HBA maximum speed is 16 GB. The highest common speed in this case is 16 GB, so the port should be configured for a speed of 16 GB.

```
FC_switch_A_1:admin> portcfgspeed 6 16

FC_switch_B_1:admin> portcfgspeed 6 16
```

2. Verify the settings:

   `portcfgshow`

```
FC_switch_A_1:admin> portcfgshow

FC_switch_B_1:admin> portcfgshow
```

   In the example output, port 6 has the following settings; speed is set to 16G:

```
Ports of Slot 0                    0   1   2   3   4   5   6   7   8
-----------------------------------+---+---+---+--+---+---+---+---+--
Speed                              16G 16G 16G 16G 16G 16G 16G 16G 16G
AL_PA Offset 13                    ..  ..  ..  ..  ..  ..  ..  ..  ..
Trunk Port                         ..  ..  ..  ..  ..  ..  ..  ..  ..
Long Distance                      ..  ..  ..  ..  ..  ..  ..  ..  ..
VC Link Init                       ..  ..  ..  ..  ..  ..  ..  ..  ..
Locked L_Port                      -   -   -   -   -  -   -   -   -
Locked G_Port                      ..  ..  ..  ..  ..  ..  ..  ..  ..
Disabled E_Port                    ..  ..  ..  ..  ..  ..  ..  ..  ..
Locked E_Port                      ..  ..  ..  ..  ..  ..  ..  ..  ..
ISL R_RDY Mode                     ..  ..  ..  ..  ..  ..  ..  .. ..
RSCN Suppressed                    ..  ..  ..  ..  ..  ..  ..  .. ..
Persistent Disable                 ..  ..  ..  ..  ..  ..  ..  .. ..
LOS TOV enable                     ..  ..  ..  ..  ..  ..  ..  .. ..
NPIV capability                    ON  ON  ON  ON  ON  ON  ON  ON  ON
NPIV PP Limit                      126 126 126 126 126 126 126 126 126
QOS Port                           AE  AE  AE  AE  AE  AE  AE  AE  ON
EX Port                            ..  ..  ..  ..  ..  ..  ..  ..  ..
Mirror Port                        ..  ..  ..  ..  ..  ..  ..  ..  ..
Rate Limit                         ..  ..  ..  ..  ..  ..  ..  ..  ..
Credit Recovery                    ON  ON  ON  ON  ON  ON  ON  ON  ON
Fport Buffers                      ..  ..  ..  ..  ..  ..  ..  ..  ..
Eport Credits                      ..  ..  ..  ..  ..  ..  ..  ..  ..
Port Auto Disable                  ..  ..  ..  ..  ..  ..  ..  ..  ..
CSCTL mode                         ..  ..  ..  ..  ..  ..  ..  ..  ..
D-Port mode                        ..  ..  ..  ..  ..  ..  ..  ..  ..
D-Port over DWDM                   ..  ..  ..  ..  ..  ..  ..  ..  ..
FEC                                ON  ON  ON  ON  ON  ON  ON  ON  ON
Fault Delay                        0   0   0   0   0   0   0   0   0
Non-DFE                            ..  ..  ..  ..  ..  ..  ..  ..  ..
```

Configuring compression on ISL ports on a Brocade G620 switch

If you are using Brocade G620 switches and enabling compression on the ISLs, you must configure it on each E-port on the switches.

About this task

This task must be performed on the ISL ports on both switches using the ISL.

Steps

1. Disable the port on which you want to configure compression:

   ```
   portdisable port-id
   ```

2. Enable compression on the port:

```
portCfgCompress --enable port-id
```

3. Enable the port to activate the configuration with compression:

```
portenable port-id
```

4. Confirm that the setting has been changed:

```
portcfgshow port-id
```

The following example enables compression on port 0.

```
FC_switch_A_1:admin> portdisable 0
FC_switch_A_1:admin> portcfgcompress --enable 0
FC_switch_A_1:admin> portenable 0
FC_switch_A_1:admin> portcfgshow 0
Area Number: 0
Octet Speed Combo: 3(16G,10G)
(output truncated)
D-Port mode: OFF
D-Port over DWDM ..
Compression: ON
Encryption: ON
```

You can use the islShow command to check that the E_port has come online with encryption or compression configured and active.

```
FC_switch_A_1:admin> islshow
  1: 0-> 0 10:00:c4:f5:7c:8b:29:86   5 FC_switch_B_1
sp: 16.000G bw: 16.000G TRUNK QOS CR_RECOV ENCRYPTION COMPRESSION
```

You can use the portEncCompShow command to see which ports are active. In this example you can see that encryption and compression are configured and active on port 0.

```
FC_switch_A_1:admin> portenccompshow
User      Encryption                   Compression           Config
Port   Configured    Active   Configured   Active  Speed
----   ----------    -------  ----------   ------  -----
  0    Yes            Yes        Yes             Yes        16G
```

Configuring zoning on Brocade FC switches

You must assign the switch ports to separate zones to separate controller and storage traffic. The procedure differs depending on whether you are using a FibreBridge 7500N or FibreBridge 6500N bridge.

Zoning for FC-VI ports

For each DR group in the MetroCluster, you must configure two zones for the FC-VI connections that allow controller-to-controller traffic. These zones contain the FC switch ports connecting to the controller module FC-VI ports. These zones are Quality of Service (QoS) zones.

A QoS zone name starts with the prefix QOSHid_, followed by a user-defined string to differentiate it from a regular zone. These QoS zones are the same regardless of the model of FibreBridge bridge that is being used.

Each zone contains all the FC-VI ports, one for each FC-VI cable from each controller. These zones are configured for high priority.

The following tables show the FC-VI zones for two DR groups.

DR group 1 : QOSH1 FC-VI zone for FC-VI port a / c

FC switch	Site	Switch domain	6505 / 6510 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	0	0	0	controller_A_1 port FC-VI a
FC_switch_A_1	A	5	1	1	1	controller_A_1 port FC-VI c
FC_switch_A_1	A	5	4	4	4	controller_A_2 port FC-VI a
FC_switch_A_1	A	5	5	5	5	controller_A_2 port FC-VI c
FC_switch_B_1	B	7	0	0	0	controller_B_1 port FC-VI a
FC_switch_B_1	B	7	1	1	1	controller_B_1 port FC-VI c
FC_switch_B_1	B	7	4	4	4	controller_B_2 port FC-VI a
FC_switch_B_1	B	7	5	5	5	controller_B_2 port FC-VI c

Zone in Fabric_1	Member ports
QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5

DR group 1 : QOSH1 FC-VI zone for FC-VI port b / d

FC switch	Site	Switch domain	6505 / 6510 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	0	0	0	controller_A_1 port FC-VI b
			1	1	1	controller_A_1 port FC-VI d

FC switch	Site	Switch domain	6505 / 6510 port	6520 port	G620 port	Connects to…
			4	4	4	controller_A_2 port FC-VI b
			5	5	5	controller_A_2 port FC-VI d
FC_switch_B_2	B	8	0	0	0	controller_B_1 port FC-VI b
			1	1	1	controller_B_1 port FC-VI d
			4	4	4	controller_B_2 port FC-VI b
			5	5	5	controller_B_2 port FC-VI d

Zone in Fabric_1	Member ports
QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5

DR group 2 : QOSH2 FC-VI zone for FC-VI port a / c

FC switch	Site	Switch domain	Switch port			Connects to…
			6510	6520	G620	
FC_switch_A_1	A	5	24	48	18	controller_A_3 port FC-VI a
			25	49	19	controller_A_3 port FC-VI c
			28	52	22	controller_A_4 port FC-VI a
			29	53	23	controller_A_4 port FC-VI c
FC_switch_B_1	B	7	24	48	18	controller_B_3 port FC-VI a
			25	49	19	controller_B_3 port FC-VI c
			28	52	22	controller_B_4 port FC-VI a
			29	53	23	controller_B_4 port FC-VI c

Zone in Fabric_1	Member ports
QOSH2_MC2_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29

QOSH2_MC2_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53

DR group 2 : QOSH2 FC-VI zone for FC-VI port b / d

FC switch	Site	Switch domain	6510 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	24	48	18	controller_A_3 port FC-VI b
FC_switch_A_2	A	6	25	49	19	controller_A_3 port FC-VI d
FC_switch_A_2	A	6	28	52	22	controller_A_4 port FC-VI b
FC_switch_A_2	A	6	29	53	23	controller_A_4 port FC-VI d
FC_switch_B_2	B	8	24	48	18	controller_B_3 port FC-VI b
FC_switch_B_2	B	8	25	49	19	controller_B_3 port FC-VI d
FC_switch_B_2	B	8	28	52	22	controller_B_4 port FC-VI b
FC_switch_B_2	B	8	29	53	23	controller_B_4 port FC-VI d

Zone in Fabric_2	Member ports
QOSH2_MC2_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29
QOSH2_MC2_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53

The following table provides a summary of the FC-VI zones:

Fabric	Zone name	Member ports
FC_switch_A_1 and FC_switch_B_1	QOSH1_MC1_FAB_1_FCVI	5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
	QOSH2_MC1_FAB_1_FCVI (6510)	5,24;5,25;5,28;5,29;7,24;7,25;7,28;7,29
	QOSH2_MC1_FAB_1_FCVI (6520)	5,48;5,49;5,52;5,53;7,48;7,49;7,52;7,53

FC_switch_A_2 and FC_switch_B_2	QOSH1_MC1_FAB_2_FCVI	6,0;6,1;6,4;6,5;8,0;8,1;8,4;8,5
	QOSH2_MC1_FAB_2_FCVI (6510)	6,24;6,25;6,28;6,29;8,24;8,25;8,28;8,29
	QOSH2_MC1_FAB_2_FCVI (6520)	6,48;6,49;6,52;6,53;8,48;8,49;8,52;8,53

Zoning for FibreBridge 6500N bridges, or FibreBridge 7500N or 7600N bridges using one FC port

If you are using FibreBridge 6500N bridges, or FibreBridge 7500N or 7600N bridges using only one of the two FC ports, you need to create storage zones for the bridge ports. You should understand the zones and associated ports before you configure the zones.

The examples show zoning for DR group 1 only. If your configuration includes a second DR group, configure the zoning for the second DR group in the same manner, using the corresponding ports of the controllers and bridges.

Required zones

You must configure one zone for each of the FC-to-SAS bridge FC ports that allows traffic between initiators on each controller module and that FC-to-SAS bridge.

Each storage zone contains nine ports:

- Eight HBA initiator ports (two connections for each controller)
- One port connecting to an FC-to-SAS bridge FC port

The storage zones use standard zoning.

The examples show two pairs of bridges connecting two stack groups at each site. Because each bridge uses one FC port, there are a total of four storage zones per fabric (eight in total).

Bridge naming

The bridges use the following example naming: bridge_site_stack grouplocation in pair

This portion of the name…	Identifies the…	Possible values…
site	Site on which the bridge pair physically resides.	A or B

stack group	Number of the stack group to which the bridge pair connects. • FibreBridge 7600N or 7500N bridges support up to four stacks in the stack group. The stack group can contain no more than 10 storage shelves. • FibreBridge 6500N bridges support only a single stack in the stack group.	1, 2, etc.
location in pair	Bridge within the bridge pair.A pair of bridges connect to a specific stack group.	a or b

Example bridge names for one stack group on each site:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

DR Group 1 - Stack 1 at Site_A

DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	5	2	controller_A_1 port 0a
FC_switch_A_1	A	5	3	controller_A_1 port 0c
FC_switch_A_1	A	5	6	controller_A_2 port 0a
FC_switch_A_1	A	5	7	controller_A_2 port 0c
FC_switch_A_1	A	5	8	bridge_A_1a FC1
FC_switch_B_1	B	7	2	controller_B_1 port 0a
FC_switch_B_1	B	7	3	controller_B_1 port 0c

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_B_1	B	7	6	controller_B_2 port 0a
FC_switch_B_1	B	7	7	controller_B_2 port 0c

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8

DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	6	2	controller_A_1 port 0b
FC_switch_A_1	A	6	3	controller_A_1 port 0d
FC_switch_A_1	A	6	6	controller_A_2 port 0b
FC_switch_A_1	A	6	7	controller_A_2 port 0d
FC_switch_A_1	A	6	8	bridge_A_1b FC1
FC_switch_B_1	B	8	2	controller_B_1 port 0b
FC_switch_B_1	B	8	3	controller_B_1 port 0d
FC_switch_B_1	B	8	6	controller_B_2 port 0b
FC_switch_B_1	B	8	7	controller_B_2 port 0d

Zone in Fabric_2	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8

DR Group 1 - Stack 2 at Site_A

DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	5	2	controller_A_1 port 0a
FC_switch_A_1	A	5	3	controller_A_1 port 0c
FC_switch_A_1	A	5	6	controller_A_2 port 0a
FC_switch_A_1	A	5	7	controller_A_2 port 0c
FC_switch_A_1	A	5	9	bridge_A_2a FC1
FC_switch_B_1	B	7	2	controller_B_1 port 0a
FC_switch_B_1	B	7	3	controller_B_1 port 0c
FC_switch_B_1	B	7	6	controller_B_2 port 0a
FC_switch_B_1	B	7	7	controller_B_2 port 0c

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9

DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	6	2	controller_A_1 port 0b
FC_switch_A_1	A	6	3	controller_A_1 port 0d
FC_switch_A_1	A	6	6	controller_A_2 port 0b
FC_switch_A_1	A	6	7	controller_A_2 port 0d
FC_switch_A_1	A	6	9	bridge_A_2b FC1
FC_switch_B_1	B	8	2	controller_B_1 port 0b
FC_switch_B_1	B	8	3	controller_B_1 port 0d

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_B_1	B	8	6	controller_B_2 port 0b
FC_switch_B_1	B	8	7	controller_B_2 port 0d

Zone in Fabric_2	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9

DR Group 1 - Stack 1 at Site_B

MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch	Connects to…
FC_switch_A_1	A	5	2	controller_A_1 port 0a
FC_switch_A_1	A	5	3	controller_A_1 port 0c
FC_switch_A_1	A	5	6	controller_A_2 port 0a
FC_switch_A_1	A	5	7	controller_A_2 port 0c
FC_switch_B_1	B	7	2	controller_B_1 port 0a
FC_switch_B_1	B	7	3	controller_B_1 port 0c
FC_switch_B_1	B	7	6	controller_B_2 port 0a
FC_switch_B_1	B	7	7	controller_B_2 port 0c
FC_switch_B_1	B	7	8	bridge_B_1a FC1

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8

DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch	Connects to…
FC_switch_A_1	A	6	2	controller_A_1 port 0b
FC_switch_A_1	A	6	3	controller_A_1 port 0d
FC_switch_A_1	A	6	6	controller_A_2 port 0b
FC_switch_A_1	A	6	7	controller_A_2 port 0d
FC_switch_B_1	B	8	2	controller_B_1 port 0b
FC_switch_B_1	B	8	3	controller_B_1 port 0d
FC_switch_B_1	B	8	6	controller_B_2 port 0b
FC_switch_B_1	B	8	7	controller_B_2 port 0d
FC_switch_B_1	B	8	8	bridge_B_1b FC1

Zone in Fabric_2	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;8,8

DR Group 1 - Stack 2 at Site_B

DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	5	2	controller_A_1 port 0a
FC_switch_A_1	A	5	3	controller_A_1 port 0c
FC_switch_A_1	A	5	6	controller_A_2 port 0a
FC_switch_A_1	A	5	7	controller_A_2 port 0c
FC_switch_B_1	B	7	2	controller_B_1 port 0a
FC_switch_B_1	B	7	3	controller_B_1 port 0c

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_B_1	B	7	6	controller_B_2 port 0a
FC_switch_B_1	B	7	7	controller_B_2 port 0c
FC_switch_B_1	B	7	9	bridge_b_2a FC1

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_b_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9

DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1:

FC switch	Site	Switch domain	Brocade 6505, 6510, 6520, G620, or G610 switch port	Connects to…
FC_switch_A_1	A	6	2	controller_A_1 port 0b
FC_switch_A_1	A	6	3	controller_A_1 port 0d
FC_switch_A_1	A	6	6	controller_A_2 port 0b
FC_switch_A_1	A	6	7	controller_A_2 port 0d
FC_switch_B_1	B	8	2	controller_B_1 port 0b
FC_switch_B_1	B	8	3	controller_B_1 port 0d
FC_switch_B_1	B	8	6	controller_B_2 port 0b
FC_switch_B_1	B	8	7	controller_B_2 port 0d
FC_switch_B_1	B	8	9	bridge_B_1b FC1

Zone in Fabric_2	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

Summary of storage zones

Fabric	Zone name	Member ports

FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;5,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,3;5,6;5,7;7,2;7,3;7,6;7,7;7,9
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,8
	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;6,9
	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,8
	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC1	6,2;6,3;6,6;6,7;8,2;8,3;8,6;8,7;8,9

Zoning for FibreBridge 7500N bridges using both FC ports

If you are using FibreBridge 7500N bridges with both FC ports, you need to create storage zones for the bridge ports. You should understand the zones and associated ports before you configure the zones.

Required zones

You must configure one zone for each of the FC-to-SAS bridge FC ports that allows traffic between initiators on each controller module and that FC-to-SAS bridge.

Each storage zone contains five ports:

- Four HBA initiator ports (one connection for each controller)
- One port connecting to an FC-to-SAS bridge FC port

The storage zones use standard zoning.

The examples show two pairs of bridges connecting two stack groups at each site. Because each bridge uses one FC port, there are a total of eight storage zones per fabric (sixteen in total).

Bridge naming

The bridges use the following example naming: bridge_site_stack grouplocation in pair

This portion of the name…	Identifies the…	Possible values…
site	Site on which the bridge pair physically resides.	A or B

stack group	Number of the stack group to which the bridge pair connects. • FibreBridge 7600N or 7500N bridges support up to four stacks in the stack group. The stack group can contain no more than 10 storage shelves. • FibreBridge 6500N bridges support only a single stack in the stack group.	1, 2, etc.
location in pair	Bridge within the bridge pair. A pair of bridges connect to a specific stack group.	a or b

Example bridge names for one stack group on each site:

- bridge_A_1a
- bridge_A_1b
- bridge_B_1a
- bridge_B_1b

DR Group 1 - Stack 1 at Site_A

DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610/ G620 port	6520 port	Connects to…
FC_switch_A_1	A	5	2	2	controller_A_1 port 0a
FC_switch_A_1	A	5	6	6	controller_A_2 port 0a
FC_switch_A_1	A	5	8	8	bridge_A_1a FC1
FC_switch_B_1	B	7	2	2	controller_B_1 port 0a
FC_switch_B_1	B	7	6	6	controller_B_2 port 0a

Zone in Fabric_1	Member ports

MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8

DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	3	3	3	controller_A_1 port 0c
FC_switch_A_1	A	5	7	7	7	controller_A_2 port 0c
FC_switch_A_1	A	5	9	9	9	bridge_A_1b FC1
FC_switch_B_1	B	7	3	3	3	controller_B_1 port 0c
FC_switch_B_1	B	7	7	7	7	controller_B_2 port 0c

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9

DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_1_BOT_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610	6520	G620	Connects to…
FC_switch_A_2	A	6	2	2	2	controller_A_1 port 0d
FC_switch_A_2	A	6	6	6	6	controller_A_2 port 0d
FC_switch_A_2	A	6	8	8	8	bridge_A_1a FC2
FC_switch_B_2	B	8	2	2	2	controller_B_1 port 0b
FC_switch_B_2	B	8	6	6	6	controller_B_2 port 0b

Zone in Fabric_1	Member ports

MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8

DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610	6520	G620	Connects to…
FC_switch_A_2	A	6	3	3	3	controller_A_1 port 0d
FC_switch_A_2	A	6	7	7	7	controller_A_2 port 0d
FC_switch_A_2	A	6	9	9	9	bridge_A_1b FC2
FC_switch_B_2	B	8	3	3	3	controller_B_1 port 0b
FC_switch_B_2	B	8	7	7	7	controller_B_2 port 0b

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9

DR Group 1 - Stack 2 at Site_A

DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	2	2	2	controller_A_1 port 0a
FC_switch_A_1	A	5	6	6	6	controller_A_2 port 0a
FC_switch_A_1	A	5	10	10	10	bridge_A_2a FC1
FC_switch_B_1	B	7	2	2	2	controller_B_1 port 0a
FC_switch_B_1	B	7	6	6	6	controller_B_2 port 0a

Zone in Fabric_1 hh	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10

DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	3	3	3	controller_A_1 port 0c
FC_switch_A_1	A	5	7	7	7	controller_A_2 port 0c
FC_switch_A_1	A	5	11	11	11	bridge_A_2b FC1
FC_switch_B_1	B	7	3	3	3	controller_B_1 port 0c
FC_switch_B_1	B	7	7	7	7	controller_B_2 port 0c

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11

DrGroup 1 : MC1_INIT_GRP_1_SITE_A_STK_GRP_2_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	2	0	0	controller_A_1 port 0b
FC_switch_A_2	A	6	6	4	4	controller_A_2 port 0b
FC_switch_A_2	A	6	10	10	10	bridge_A_2a FC2
FC_switch_B_2	B	8	2	2	2	controller_B_1 port 0b
FC_switch_B_2	B	8	6	6	6	controller_B_2 port 0b

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10

DrGroup 1 : MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	3	3	3	controller_A_1 port 0b
FC_switch_A_2	A	6	7	7	7	controller_A_2 port 0b
FC_switch_A_2	A	6	11	11	11	bridge_A_2b FC2
FC_switch_B_2	B	8	3	3	3	controller_B_1 port 0b\
FC_switch_B_2	B	8	7	7	7	controller_B_2 port 0b

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11

DR Group 1 - Stack 1 at Site_B

DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	2	2	2	controller_A_1 port 0a
FC_switch_A_1	A	5	6	6	6	controller_A_2 port 0a
FC_switch_B_1	B	7	2	2	8	controller_B_1 port 0a
FC_switch_B_1	B	7	6	6	2	controller_B_2 port 0a

FC_switch_B_1	B	7	8	8	6	bridge_B_1a FC1

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8

DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	3	3	3	controller_A_1 port 0c
FC_switch_A_1	A	5	7	7	7	controller_A_2 port 0c
FC_switch_B_1	B	7	3	3	9	controller_B_1 port 0c
FC_switch_B_1	B	7	7	7	3	controller_B_2 port 0c
FC_switch_B_1	B	7	9	9	7	bridge_B_1b FC1

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9

DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_1_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	2	2	2	controller_A_1 port 0b
FC_switch_A_2	A	6	6	6	6	controller_A_2 port 0b
FC_switch_B_2	B	8	2	2	2	controller_B_1 port 0b
FC_switch_B_2	B	8	6	6	6	controller_B_2 port 0b

FC_switch_B_2	B	8	8	8	8	bridge_B_1a FC2

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8

DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	3	3	3	controller_A_1 port 0b
FC_switch_A_2	A	6	7	7	7	controller_A_2 port 0b
FC_switch_B_2	B	8	3	3	3	controller_B_1 port 0b
FC_switch_B_2	B	8	7	7	7	controller_B_2 port 0b
FC_switch_B_2	B	8	9	9	9	bridge_A_1b FC2

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9

DR Group 1 - Stack 2 at Site_B

DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_1	A	5	2	2	2	controller_A_1 port 0a
FC_switch_A_1	A	5	6	6	6	controller_A_2 port 0a
FC_switch_B_1	B	7	2	2	2	controller_B_1 port 0a

FC_switch_B_1	B	7	6	6	6	controller_B_2 port 0a
FC_switch_B_1	B	7	10	10	10	bridge_B_2a FC1

Zone in Fabric_1	**Member ports**
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10

DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_TOP_FC1:

FC switch	**Site**	**Switch domain**	**6505 / 6510 / G610 port**	**6520 port**	**G620 port**	**Connects to…**
FC_switch_A_1	A	5	3	3	3	controller_A_1 port 0c
FC_switch_A_1	A	5	7	7	7	controller_A_2 port 0c
FC_switch_B_1	B	7	3	3	3	controller_B_1 port 0c
FC_switch_B_1	B	7	7	7	7	controller_B_2 port 0c
FC_switch_B_1	B	7	11	11	11	bridge_B_2b FC1

Zone in Fabric_2 hh	Member ports
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11

DrGroup 1 : MC1_INIT_GRP_1_SITE_B_STK_GRP_2_BOT_FC2:

FC switch	**Site**	**Switch domain**	**6505 / 6510 / G610 port**	**6520 port**	**G620 port**	**Connects to…**
FC_switch_A_2	A	6	2	2	2	controller_A_1 port 0b
FC_switch_A_2	A	6	6	6	6	controller_A_2 port 0b
FC_switch_B_2	B	8	2	2	2	controller_B_1 port 0b

FC_switch_B_2	B	8	6	6	6	controller_B_2 port 0b
FC_switch_B_2	B	8	10	10	10	bridge_B_2a FC2

Zone in Fabric_1	Member ports
MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10

DrGroup 1 : MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2:

FC switch	Site	Switch domain	6505 / 6510 / G610 port	6520 port	G620 port	Connects to…
FC_switch_A_2	A	6	3	3	3	controller_A_1 port 0b
FC_switch_A_2	A	6	7	7	7	controller_A_2 port 0b
FC_switch_B_2	B	8	3	3	3	controller_B_1 port 0b
FC_switch_B_2	B	8	7	7	7	controller_B_2 port 0b
FC_switch_B_2	B	8	11	11	11	bridge_B_2b FC2

Zone in Fabric_2	Member ports
MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

Summary of storage zones

Fabric	Zone name	Member ports
FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;5,8
FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;5,9
FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;5,10

FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;5,11
FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC1	5,2;5,6;7,2;7,6;7,8
FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC1	5,3;5,7;7,3;7,7;7,9
FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC1	5,2;5,6;7,2;7,6;7,10
FC_switch_A_1 and FC_switch_B_1	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC1	5,3;5,7;7,3;7,7;7,11
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;6,8
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;6,9
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_1_SITE_A_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;6,10
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_2_SITE_A_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;6,11
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_1_TOP_FC2	6,2;6,6;8,2;8,6;8,8
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_1_BOT_FC2	6,3;6,7;8,3;8,7;8,9
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_1_SITE_B_STK_GRP_2_TOP_FC2	6,2;6,6;8,2;8,6;8,10
FC_switch_A_2 and FC_switch_B_2	MC1_INIT_GRP_2_SITE_B_STK_GRP_2_BOT_FC2	6,3;6,7;8,3;8,7;8,11

Configuring zoning on Brocade FC switches

You must assign the switch ports to separate zones to separate controller and storage traffic, with zones for the FC-VI ports and zones for the storage ports.

About this task

The following steps use the standard zoning for the MetroCluster configuration.

Zoning for FC-VI ports

[Zoning for FibreBridge 6500N bridges, or FibreBridge 7500N or 7600N bridges using one FC port]

[Zoning for FibreBridge 7500N bridges using both FC ports]

Steps

1. Create the FC-VI zones on each switch:

   `zonecreate "QOSH1_FCVI_1", member;member …`

   In this example a QOS FCVI zone is created containing ports 5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5:

   ```
   Switch_A_1:admin> zonecreate "QOSH1_FCVI_1",
   "5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5"
   ```

2. Configure the storage zones on each switch.

   You can configure zoning for the fabric from one switch in the fabric. In the example that follows, zoning is configured on Switch_A_1.

   a. Create the storage zone for each switch domain in the switch fabric:

      `zonecreate name, member;member …`

      In this example a storage zone for a FibreBridge 7500N using both FC ports is being created. The zones contains ports 5,2;5,6;7,2;7,6;5,16:

      ```
      Switch_A_1:admin> zonecreate
      "MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1", "5,2;5,6;7,2;7,6;5,16"
      ```

   b. Create the configuration in the first switch fabric:

      `cfgcreate config_name, zone;zone…`

      In this example a configuration with the name CFG_1 and the two zones QOSH1_MC1_FAB_1_FCVI and MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1 is created

      ```
      Switch_A_1:admin> cfgcreate "CFG_1", "QOSH1_MC1_FAB_1_FCVI;
      MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1"
      ```

   c. Add zones to the configuration, if desired:

      `cfgadd config_namezone;zone…`

   d. Enable the configuration:

      `cfgenable config_name`

```
Switch_A_1:admin> cfgenable "CFG_1"
```

e. Save the configuration:

`cfgsave`

```
Switch_A_1:admin> cfgsave
```

f. Validate the zoning configuration:

`zone --validate`

```
Switch_A_1:admin> zone --validate
Defined configuration:
cfg: CFG_1 QOSH1_MC1_FAB_1_FCVI ;
MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
zone: QOSH1_MC1_FAB_1_FCVI
5,0;5,1;5,4;5,5;7,0;7,1;7,4;7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2;5,6;7,2;7,6;5,16
Effective configuration:
cfg: CFG_1
zone: QOSH1_MC1_FAB_1_FCVI
5,0
5,1
5,4
5,5
7,0
7,1
7,4
7,5
zone: MC1_INIT_GRP_1_SITE_A_STK_GRP_1_TOP_FC1
5,2
5,6
7,2
7,6
5,16
------------------------------------
~ - Invalid configuration
* - Member does not exist
# - Invalid usage of broadcast zone
```

Setting ISL encryption on Brocade 6510 or G620 switches

On Brocade 6510 or G620 switches, you can optionally use the Brocade encryption feature on the ISL connections. If you want to use the encryption feature, you must perform additional configuration steps on each switch in the MetroCluster configuration.

Before you begin

- You must have Brocade 6510 or G620 switches.

> Support for ISL encryption on Brocade G620 switches is only supported on ONTAP 9.4 and later.

- You must have selected two switches from the same fabric.
- You must have reviewed the Brocade documentation for your switch and Fabric Operating System version to confirm the bandwidth and port limits.

About this task

The steps must be performed on both the switches in the same fabric.

Disabling virtual fabric

In order to set the ISL encryption, you must disable the virtual fabric on all the four switches being used in a MetroCluster configuration.

Steps

1. Disable the virtual fabric by entering the following command at the switch console:

   ```
   fosconfig --disable vf
   ```

2. Reboot the switch.

Setting the payload

After disabling the virtual fabric, you must set the payload or the data field size on both switches in the fabric.

About this task

The data field size must not exceed 2048.

Steps

1. Disable the switch:

   ```
   switchdisable
   ```

2. Configure and set the payload:

   ```
   configure
   ```

3. Set the following switch parameters:

   a. Set the Fabric parameter as follows: `y`

   b. Set the other parameters, such as Domain, WWN-based persistent PID, and so on.

c. Set the data field size: `2048`

Setting the authentication policy

You must set the authentication policy and associated parameters.

About this task

The commands must be executed at the switch console.

Steps

1. Set the authentication secret:

   a. Begin the setup process:

   ```
   secAuthSecret --set
   ```

   This command initiates a series of prompts that you respond to in the following steps:

   b. Provide the worldwide name (WWN) of the other switch in the fabric for the "Enter peer WWN, Domain, or switch name" parameter.

   c. Provide the peer secret for the "Enter peer secret" parameter.

   d. Provide the local secret for the "Enter local secret" parameter.

   e. Enter `Y` for the "Are you done" parameter.

   The following is an example of setting the authentication secret:

```
brcd> secAuthSecret --set

This command is used to set up secret keys for the DH-CHAP
authentication.
The minimum length of a secret key is 8 characters and maximum 40
characters. Setting up secret keys does not initiate DH-CHAP
authentication. If switch is configured to do DH-CHAP, it is
performed
whenever a port or a switch is enabled.

Warning: Please use a secure channel for setting secrets. Using
an insecure channel is not safe and may compromise secrets.

Following inputs should be specified for each entry.

1. WWN for which secret is being set up.
2. Peer secret: The secret of the peer that authenticates to peer.
3. Local secret: The local secret that authenticates peer.

Press enter to start setting up secrets > <cr>

Enter peer WWN, Domain, or switch name (Leave blank when done):
10:00:00:05:33:76:2e:99
Enter peer secret: <hidden>
Re-enter peer secret: <hidden>
Enter local secret: <hidden>
Re-enter local secret: <hidden>

Enter peer WWN, Domain, or switch name (Leave blank when done):
Are you done? (yes, y, no, n): [no] yes
Saving data to key store... Done.
```

2. Set the authentication group to 4:

   `authUtil --set -g 4`

3. Set the authentication type to "dhchap":

   `authUtil --set -a dhchap`

   The system displays the following output:

   ```
   Authentication is set to dhchap.
   ```

4. Set the authentication policy on the switch to on:

```
authUtil --policy -sw on
```

The system displays the following output:

```
Warning: Activating the authentication policy requires either DH-CHAP
secrets or PKI certificates depending on the protocol selected.
Otherwise, ISLs will be segmented during next E-port bring-up.
ARE YOU SURE  (yes, y, no, n): [no] yes
Auth Policy is set to ON
```

Enabling ISL encryption on Brocade switches

After setting the authentication policy and the authentication secret, you must enable ISL encryption on the ports for it to take effect.

About this task

- These steps should be performed on one switch fabric at a time.
- The commands must be run at the switch console.

Steps

1. Enable encryption on all of the ISL ports:

   ```
   portCfgEncrypt --enable port_number
   ```

   In the following example, the encryption is enabled on ports 8 and 12:

   ```
   portCfgEncrypt --enable 8
   ```

   ```
   portCfgEncrypt --enable 12
   ```

2. Enable the switch:

   ```
   switchenable
   ```

3. Verify that the ISL is up and working:

   ```
   islshow
   ```

4. Verify that encryption is enabled:

   ```
   portenccompshow
   ```

   The following example shows that encryption is enabled on ports 8 and 12:

```
User Encryption
Port  configured     Active
----   ----------    ------
 8      yes           yes
 9      No            No
 10     No            No
 11     No            No
 12     yes           yes
```

What to do next

Perform all of the steps on the switches in the other fabric in a MetroCluster configuration.

Configuring the Cisco FC switches manually

Each Cisco switch in the MetroCluster configuration must be configured appropriately for the ISL and storage connections.

Before you begin

The following requirements apply to the Cisco FC switches:

- You must be using four supported Cisco switches of the same model with the same NX-OS version and licensing.
- The MetroCluster configuration requires four switches.

  The four switches must be connected into two fabrics of two switches each, with each fabric spanning both sites.

- The switch must support connectivity to the ATTO FibreBridge model.
- You cannot be using encryption or compression in the Cisco FC storage fabric. It is not supported in the MetroCluster configuration.

In the NetApp Interoperability Matrix Tool (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 following requirement applies to the Inter-Switch Link (ISL) connections:

- All ISLs must have the same length and same speed in one fabric.

  Different lengths of ISLs can be used in the different fabrics. The same speed must be used in all fabrics.

The following requirement applies to the storage connections:

- Each storage controller must have four initiator ports available to connect to the switch fabrics.

  Two initiator ports must be connected from each storage controller to each fabric.

> You can configure FAS8020, AFF8020, FAS8200, and AFF A300 systems with two initiators ports per controller (a single initiator port to each fabric) if all of the following criteria are met:
>
> - There are fewer than four FC initiator ports available to connect the disk storage and no additional ports can be configured as FC initiators.
> - All slots are in use and no FC initiator card can be added.

Related information

NetApp Interoperability Matrix Tool

Cisco switch license requirements

Certain feature-based licenses might be required for the Cisco switches in a fabric-attached MetroCluster configuration. These licenses enable you to use features such as QoS or long-distance mode credits on the switches. You must install the required feature-based licenses on all four switches in a MetroCluster configuration.

The following feature-based licenses might be required in a MetroCluster configuration:

- ENTERPRISE_PKG

  This license enables you to use the QoS feature on Cisco switches.

- PORT_ACTIVATION_PKG

  You can use this license for Cisco 9148 switches. This license enables you to activate or deactivate ports on the switches as long as only 16 ports are active at any given time. By default, 16 ports are enabled in Cisco MDS 9148 switches.

- FM_SERVER_PKG

  This license enables you to manage fabrics simultaneously and to manage switches through a web browser.

  The FM_SERVER_PKG license also enables performance management features such as performance thresholds and threshold monitoring. For more information about this license, see the Cisco Fabric Manager Server Package.

You can verify that the licenses are installed by using the show license usage command. If you do not have these licenses, contact your sales representative before proceeding with the installation.

> The Cisco MDS 9250i switches have two fixed 1/10 GbE IP storage services ports. No additional licenses are required for these ports. The Cisco SAN Extension over IP application package is a standard license on these switches that enables features such as FCIP and compression.

Setting the Cisco FC switch to factory defaults

To ensure a successful configuration, you must set the switch to its factory defaults. This ensures that the switch is starting from a clean configuration.

About this task

This task must be performed on all switches in the MetroCluster configuration.

Steps

1. Make a console connection and log in to both switches in the same fabric.
2. Issue the following command to set the switch back to its default settings:

   `write erase`

   You can respond `y` when prompted to confirm the command. This erases all licenses and configuration information on the switch.

3. Issue the following command to reboot the switch:

   `reload`

   You can respond `y` when prompted to confirm the command.

4. Repeat the `write erase` and `reload` commands on the other switch.

   After issuing the `reload` command, the switch reboots and then prompts with setup questions. At that point, proceed to the next section.

Example

The following example shows the process on a fabric consisting of FC_switch_A_1 and FC_switch_B_1.

```
FC_Switch_A_1# write erase
    Warning: This command will erase the startup-configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_A_1# reload
    This command will reboot the system. (y/n)?  [n] y

FC_Switch_B_1# write erase
    Warning: This command will erase the startup-configuration.
    Do you wish to proceed anyway? (y/n)  [n] y
    FC_Switch_B_1# reload
    This command will reboot the system. (y/n)?  [n] y
```

Configure the Cisco FC switch basic settings and community string

You must specify the basic settings with the `setup` command or after issuing the `reload` command.

Steps

1. If the switch does not display the setup questions, configure the basic switch settings:

   `setup`

2. Accept the default responses to the setup questions until you are prompted for the SNMP community string.
3. Set the community string to "public" (all lowercase) to allow access from the ONTAP Health Monitors.

   You can set the community string to a value other than "public", but you must configure the ONTAP Health Monitors using the community string you specify.

   The following example shows the commands on FC_switch_A_1:

```
FC_switch_A_1# setup
    Configure read-only SNMP community string (yes/no) [n]: y
    SNMP community string : public
    Note:  Please set the SNMP community string to "Public" or another
value of your choosing.
    Configure default switchport interface state (shut/noshut) [shut]:
noshut
    Configure default switchport port mode F (yes/no) [n]: n
    Configure default zone policy (permit/deny) [deny]: deny
    Enable full zoneset distribution? (yes/no) [n]: yes
```

   The following example shows the commands on FC_switch_B_1:

```
FC_switch_B_1# setup
    Configure read-only SNMP community string (yes/no) [n]: y
    SNMP community string : public
    Note:  Please set the SNMP community string to "Public" or another
value of your choosing.
    Configure default switchport interface state (shut/noshut) [shut]:
noshut
    Configure default switchport port mode F (yes/no) [n]: n
    Configure default zone policy (permit/deny) [deny]: deny
    Enable full zoneset distribution? (yes/no) [n]: yes
```

Acquiring licenses for ports

You do not have to use Cisco switch licenses on a continuous range of ports; instead, you can acquire licenses for specific ports that are used and remove licenses from unused ports.

Before you begin

You should verify the number of licensed ports in the switch configuration and, if necessary, move licenses from one port to another as needed.

Steps

1. Issue the following command to show license usage for a switch fabric:

```
show port-resources module 1
```

Determine which ports require licenses. If some of those ports are unlicensed, determine if you have extra licensed ports and consider removing the licenses from them.

2. Issue the following command to enter configuration mode:

   ```
   config t
   ```

3. Remove the license from the selected port:
   a. Issue the following command to select the port to be unlicensed:

      ```
      interface interface-name
      ```

   b. Remove the license from the port:

      ```
      no port-license acquire
      ```

   c. Exit the port configuration interface:

      ```
      exit
      ```

4. Acquire the license for the selected port:
   a. Issue the following command to select the port to be unlicensed:

      ```
      interface interface-name
      ```

   b. Make the port eligible to acquire a license:

      ```
      port-license
      ```

   c. Acquire the license on the port:

      ```
      port-license acquire
      ```

   d. Exit the port configuration interface:

      ```
      exit
      ```

5. Repeat for any additional ports.
6. Exit configuration mode:

   ```
   exit
   ```

Removing and acquiring a license on a port

This example shows a license being removed from port fc1/2, port fc1/1 being made eligible to acquire a license, and the license being acquired on port fc1/1:

```
Switch_A_1# conf t
    Switch_A_1(config)# interface fc1/2
    Switch_A_1(config)# shut
    Switch_A_1(config-if)# no port-license acquire
    Switch_A_1(config-if)# exit
    Switch_A_1(config)# interface fc1/1
    Switch_A_1(config-if)# port-license
    Switch_A_1(config-if)# port-license acquire
    Switch_A_1(config-if)# no shut
    Switch_A_1(config-if)# end
    Switch_A_1# copy running-config startup-config

    Switch_B_1# conf t
    Switch_B_1(config)# interface fc1/2
    Switch_B_1(config)# shut
    Switch_B_1(config-if)# no port-license acquire
    Switch_B_1(config-if)# exit
    Switch_B_1(config)# interface fc1/1
    Switch_B_1(config-if)# port-license
    Switch_B_1(config-if)# port-license acquire
    Switch_B_1(config-if)# no shut
    Switch_B_1(config-if)# end
    Switch_B_1# copy running-config startup-config
```

The following example shows port license usage being verified:

```
Switch_A_1# show port-resources module 1
    Switch_B_1# show port-resources module 1
```

Enabling ports in a Cisco MDS 9148 or 9148S switch

In Cisco MDS 9148 or 9148S switches, you must manually enable the ports required in a MetroCluster configuration.

About this task

- You can manually enable 16 ports in a Cisco MDS 9148 or 9148S switch.
- The Cisco switches enable you to apply the POD license on random ports, as opposed to applying them in sequence.
- Cisco switches require that you use one port from each port group, unless you need more than 12 ports.

Steps

1. View the port groups available in a Cisco switch:

   `show port-resources module` *`blade_number`*

2. License and acquire the required port in a port group by entering the following commands in sequence:

   `config t`

   `interface port_number`

   `shut`

   `port-license acquire`

   `no shut`

   For example, the following command sequence licenses and acquires Port fc 1/45:

   ```
   switch# config t
   switch(config)#
   switch(config)# interface fc 1/45
   switch(config-if)#
   switch(config-if)# shut
   switch(config-if)# port-license acquire
   switch(config-if)# no shut
   switch(config-if)# end
   ```

3. Save the configuration:

   `copy running-config startup-config`

Configuring the F-ports on a Cisco FC switch

You must configure the F-ports on the FC switch.

About this task

In a MetroCluster configuration, the F-ports are the ports that connect the switch to the HBA initiators, FC-VI interconnects and FC-to-SAS bridges.

Each port must be configured individually.

Refer to the following sections to identify the F-ports (switch-to-node) for your configuration:

- Port assignments for FC switches when using ONTAP 9.1 and later
- Port assignments for FC switches when using ONTAP 9.0

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

Steps

1. Issue the following command to enter configuration mode:

   `config t`

2. Enter interface configuration mode for the port:

   `interface port-ID`

3. Shut down the port:

   `shutdown`

4. Set the ports to F mode by issuing the following command:

   `switchport mode F`

5. Set the ports to fixed speed by issuing the following command:

   `switchport speed speed-value`

   speed-value is either `8000` or `16000`

6. Set the rate mode of the switch port to dedicated by issuing the following command:

   `switchport rate-mode dedicated`

7. Restart the port:

   `no shutdown`

8. Issue the following command to exit configuration mode:

   `end`

Example

The following example shows the commands on the two switches:

```
Switch_A_1# config  t
FC_switch_A_1(config)# interface fc 1/1
FC_switch_A_1(config-if)# shutdown
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport speed 8000
FC_switch_A_1(config-if)# switchport rate-mode dedicated
FC_switch_A_1(config-if)# no shutdown
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# config  t
FC_switch_B_1(config)# interface fc 1/1
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport speed 8000
FC_switch_B_1(config-if)# switchport rate-mode dedicated
FC_switch_B_1(config-if)# no shutdown
FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

Assigning buffer-to-buffer credits to F-Ports in the same port group as the ISL

You must assign the buffer-to-buffer credits to the F-ports if they are in the same port group as the ISL. If the ports do not have the required buffer-to-buffer credits, the ISL could be inoperative.

About this task

This task is not required if the F-ports are not in the same port group as the ISL port.

If the F-Ports are in a port group that contains the ISL, this task must be performed on each FC switch in the MetroCluster configuration.

Steps

1. Enter configuration mode:

   `config t`

2. Set the interface configuration mode for the port:

   `interface` *`port-ID`*

3. Disable the port:

   `shut`

4. If the port is not already in F mode, set the port to F mode:

   `switchport mode F`

5. Set the buffer-to-buffer credit of the non-E ports to 1:

```
switchport fcrxbbcredit 1
```

6. Re-enable the port:

```
no shut
```

7. Exit configuration mode:

```
exit
```

8. Copy the updated configuration to the startup configuration:

```
copy running-config startup-config
```

9. Verify the buffer-to-buffer credit assigned to a port:

```
show port-resources module 1
```

10. Exit configuration mode:

```
exit
```

11. Repeat these steps on the other switch in the fabric.
12. Verify the settings:

```
show port-resource module 1
```

Example

In this example, port fc1/40 is the ISL. Ports fc1/37, fc1/38 and fc1/39 are in the same port group and must be configured.

The following commands show the port range being configured for fc1/37 through fc1/39:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/37-39
FC_switch_A_1(config-if)# shut
FC_switch_A_1(config-if)# switchport mode F
FC_switch_A_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/37-39
FC_switch_B_1(config-if)# shut
FC_switch_B_1(config-if)# switchport mode F
FC_switch_B_1(config-if)# switchport fcrxbbcredit 1
FC_switch_A_1(config-if)# no shut
FC_switch_A_1(config-if)# exit
FC_switch_B_1# copy running-config startup-config
```

The following commands and system output show that the settings are properly applied:

```
FC_switch_A_1# show port-resource module 1
...
Port-Group 11
 Available dedicated buffers are 93

--------------------------------------------------------------------
Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                      Buffers     (Gbps)

--------------------------------------------------------------------
fc1/37                                     32        8.0  dedicated
fc1/38                                      1        8.0  dedicated
fc1/39                                      1        8.0  dedicated
...

FC_switch_B_1# port-resource module
...
Port-Group 11
 Available dedicated buffers are 93

--------------------------------------------------------------------
Interfaces in the Port-Group       B2B Credit  Bandwidth  Rate Mode
                                     Buffers     (Gbps)

--------------------------------------------------------------------
fc1/37                                     32        8.0  dedicated
fc1/38                                      1        8.0  dedicated
fc1/39                                      1        8.0 dedicated
...
```

Creating and configuring VSANs on Cisco FC switches

You must create a VSAN for the FC-VI ports and a VSAN for the storage ports on each FC switch in the MetroCluster configuration.

About this task

The VSANs should have a unique number and name. You must do additional configuration if you are using two ISLs with in-order delivery of frames.

The examples of this task use the following naming conventions:

Switch fabric	VSAN name	ID number
1	FCVI_1_10	10
	STOR_1_20	20

2	FCVI_2_30	30
	STOR_2_20	40

This task must be performed on each FC switch fabric.

Steps

1. Configure the FC-VI VSAN:
   a. Enter configuration mode if you have not done so already:

      ```
      config t
      ```

   b. Edit the VSAN database:

      ```
      vsan database
      ```

   c. Set the VSAN ID:

      ```
      vsan vsan-ID
      ```

   d. Set the VSAN name:

      ```
      vsan vsan-ID name vsan_name
      ```

2. Add ports to the FC-VI VSAN:
   a. Add the interfaces for each port in the VSAN:

      ```
      vsan vsan-ID interface interface_name
      ```

      For the FC-VI VSAN, the ports connecting the local FC-VI ports will be added.

   b. Exit configuration mode:

      ```
      end
      ```

   c. Copy the running-config to the startup-config:

      ```
      copy running-config startup-config
      ```

      In the following example, the ports are fc1/1 and fc1/13:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 10 interface fc1/1
FC_switch_A_1(config)# vsan 10 interface fc1/13
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 10 interface fc1/1
FC_switch_B_1(config)# vsan 10 interface fc1/13
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

3. Verify port membership of the VSAN:

   `show vsan member`

```
FC_switch_A_1# show vsan member
FC_switch_B_1# show vsan member
```

4. Configure the VSAN to guarantee in-order delivery of frames or out-of-order delivery of frames:

   > The standard IOD settings are recommended. You should configure OOD only if necessary.

   Considerations for using TDM/WDM equipment with fabric-attached MetroCluster configurations

   - The following steps must be performed to configure in-order delivery of frames:

     a. Enter configuration mode:

        `conf t`

     b. Enable the in-order guarantee of exchanges for the VSAN:

        `in-order-guarantee vsan` *`vsan-ID`*

        > For FC-VI VSANs (FCVI_1_10 and FCVI_2_30), you must enable in-order guarantee of frames and exchanges only on VSAN 10.

     c. Enable load balancing for the VSAN:

        `vsan` *`vsan-ID`* `loadbalancing src-dst-id`

     d. Exit configuration mode:

        `end`

     e. Copy the running-config to the startup-config:

```
copy running-config startup-config
```

The commands to configure in-order delivery of frames on FC_switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to configure in-order delivery of frames on FC_switch_B_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

- The following steps must be performed to configure out-of-order delivery of frames:

  a. Enter configuration mode:

  ```
  conf t
  ```

  b. Disable the in-order guarantee of exchanges for the VSAN:

  ```
  no in-order-guarantee vsan vsan-ID
  ```

  c. Enable load balancing for the VSAN:

  ```
  vsan vsan-ID loadbalancing src-dst-id
  ```

  d. Exit configuration mode:

  ```
  end
  ```

  e. Copy the running-config to the startup-config:

  ```
  copy running-config startup-config
  ```

  The commands to configure out-of-order delivery of frames on FC_switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to configure out-of-order delivery of frames on FC_switch_B_1:

```
FC_switch_B_1# config t
FC_switch_B_1(config)# no in-order-guarantee vsan 10
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 10 loadbalancing src-dst-id
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

> When configuring ONTAP on the controller modules, OOD must be explicitly configured on each controller module in the MetroCluster configuration.

Configuring in-order delivery or out-of-order delivery of frames on ONTAP software

5. Set QoS policies for the FC-VI VSAN:

   a. Enter configuration mode:

      `conf t`

   b. Enable the QoS and create a class map by entering the following commands in sequence:

      `qos enable`

      `qos class-map` *`class_name`* `match-any`

   c. Add the class map created in a previous step to the policy map:

      `class` *`class_name`*

   d. Set the priority:

      `priority high`

   e. Add the VSAN to the policy map created previously in this procedure:

      `qos service policy` *`policy_name`* `vsan` *`vsan-id`*

   f. Copy the updated configuration to the startup configuration:

      `copy running-config startup-config`

The commands to set the QoS policies on FC_switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# qos enable
FC_switch_A_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_A_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_A_1(config-pmap)# class FCVI_1_10_Class
FC_switch_A_1(config-pmap-c)# priority high
FC_switch_A_1(config-pmap-c)# exit
FC_switch_A_1(config)# exit
FC_switch_A_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to set the QoS policies on FC_switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# qos enable
FC_switch_B_1(config)# qos class-map FCVI_1_10_Class match-any
FC_switch_B_1(config)# qos policy-map FCVI_1_10_Policy
FC_switch_B_1(config-pmap)# class FCVI_1_10_Class
FC_switch_B_1(config-pmap-c)# priority high
FC_switch_B_1(config-pmap-c)# exit
FC_switch_B_1(config)# exit
FC_switch_B_1(config)# qos service policy FCVI_1_10_Policy vsan 10
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

6. Configure the storage VSAN:

   a. Set the VSAN ID:

      `vsan` *`vsan-ID`*

   b. Set the VSAN name:

      `vsan` *`vsan-ID`* `name` *`vsan_name`*

The commands to configure the storage VSAN on FC_switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config-vsan-db)# vsan 20
FC_switch_A_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config
```

The commands to configure the storage VSAN on FC_switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config-vsan-db)# vsan 20
FC_switch_B_1(config-vsan-db)# vsan 20 name STOR_1_20
FC_switch_B_1(config-vsan-db)# end
FC_switch_B_1# copy running-config startup-config
```

7. Add ports to the storage VSAN.

   For the storage VSAN, all ports connecting HBA or FC-to-SAS bridges must be added. In this example fc1/5, fc1/9, fc1/17, fc1/21. fc1/25, fc1/29, fc1/33, and fc1/37 are being added.

   The commands to add ports to the storage VSAN on FC_switch_A_1:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# vsan database
FC_switch_A_1(config)# vsan 20 interface fc1/5
FC_switch_A_1(config)# vsan 20 interface fc1/9
FC_switch_A_1(config)# vsan 20 interface fc1/17
FC_switch_A_1(config)# vsan 20 interface fc1/21
FC_switch_A_1(config)# vsan 20 interface fc1/25
FC_switch_A_1(config)# vsan 20 interface fc1/29
FC_switch_A_1(config)# vsan 20 interface fc1/33
FC_switch_A_1(config)# vsan 20 interface fc1/37
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config
```

   The commands to add ports to the storage VSAN on FC_switch_B_1:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# vsan database
FC_switch_B_1(config)# vsan 20 interface fc1/5
FC_switch_B_1(config)# vsan 20 interface fc1/9
FC_switch_B_1(config)# vsan 20 interface fc1/17
FC_switch_B_1(config)# vsan 20 interface fc1/21
FC_switch_B_1(config)# vsan 20 interface fc1/25
FC_switch_B_1(config)# vsan 20 interface fc1/29
FC_switch_B_1(config)# vsan 20 interface fc1/33
FC_switch_B_1(config)# vsan 20 interface fc1/37
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

Configuring E-ports

You must configure the switch ports that connect the ISL (these are the E-Ports).

About this task

The procedure you use depends on which switch you are using:

- Configuring the E-ports on the Cisco FC switch
- Configuring FCIP ports for a single ISL on Cisco 9250i FC switches
- Configuring FCIP ports for a dual ISL on Cisco 9250i FC switches

Configuring the E-ports on the Cisco FC switch

You must configure the FC switch ports that connect the inter-switch link (ISL).

About this task

These are the E-ports, and configuration must be done for each port. To do so, you must calculate the correct number of buffer-to-buffer credits (BBCs).

All ISLs in the fabric must be configured with the same speed and distance settings.

This task must be performed on each ISL port.

Steps

1. Use the following table to determine the adjusted required BBCs per kilometer for possible port speeds.

   To determine the correct number of BBCs, you multiply the Adjusted BBCs required (determined from the following table) by the distance in kilometers between the switches. An adjustment factor of 1.5 is required to account for FC-VI framing behavior.

Speed in Gbps	BBCs required per kilometer	Adjusted BBCs required (BBCs per km x 1.5)
1	0.5	0.75

2	1	1.5
4	2	3
8	4	6
16	8	12

For example, to compute the required number of credits for a distance of 30 km on a 4-Gbps link, make the following calculation:

- `Speed in Gbps` is 4
- `Adjusted BBCs required` is 3
- `Distance in kilometers between switches` is 30 km
- 3 x 30 = 90

1. Enter configuration mode:

   ```
   config t
   ```

2. Specify the port you are configuring:

   ```
   interface port-name
   ```

3. Shut down the port:

   ```
   shutdown
   ```

4. Set the rate mode of the port to "dedicated":

   ```
   switchport rate-mode dedicated
   ```

5. Set the speed for the port:

   ```
   switchport speed speed-value
   ```

6. Set the buffer-to-buffer credits for the port:

   ```
   switchport fcrxbbcredit number_of_buffers
   ```

7. Set the port to E mode:

   ```
   switchport mode E
   ```

8. Enable the trunk mode for the port:

   ```
   switchport trunk mode on
   ```

9. Add the ISL virtual storage area networks (VSANs) to the trunk:

```
switchport trunk allowed vsan 10

switchport trunk allowed vsan add 20
```

10. Add the port to port channel 1:

```
channel-group 1
```

11. Repeat the previous steps for the matching ISL port on the partner switch in the fabric.

    The following example shows port fc1/41 configured for a distance of 30 km and 8 Gbps:

```
FC_switch_A_1# conf t
FC_switch_A_1# shutdown
FC_switch_A_1# switchport rate-mode dedicated
FC_switch_A_1# switchport speed 8000
FC_switch_A_1# switchport fcrxbbcredit 60
FC_switch_A_1# switchport mode E
FC_switch_A_1# switchport trunk mode on
FC_switch_A_1# switchport trunk allowed vsan 10
FC_switch_A_1# switchport trunk allowed vsan add 20
FC_switch_A_1# channel-group 1
fc1/36 added to port-channel 1 and disabled

FC_switch_B_1# conf t
FC_switch_B_1# shutdown
FC_switch_B_1# switchport rate-mode dedicated
FC_switch_B_1# switchport speed 8000
FC_switch_B_1# switchport fcrxbbcredit 60
FC_switch_B_1# switchport mode E
FC_switch_B_1# switchport trunk mode on
FC_switch_B_1# switchport trunk allowed vsan 10
FC_switch_B_1# switchport trunk allowed vsan add 20
FC_switch_B_1# channel-group 1
fc1/36 added to port-channel 1 and disabled
```

12. Issue the following command on both switches to restart the ports:

```
no shutdown
```

13. Repeat the previous steps for the other ISL ports in the fabric.
14. Add the native VSAN to the port-channel interface on both switches in the same fabric:

```
interface port-channel number

switchport trunk allowed vsan add native_san_id
```

15. Verify configuration of the port-channel:

```
show interface port-channel number
```

The port channel should have the following attributes:

- The port-channel is "trunking".
- Admin port mode is E, trunk mode is on.
- Speed shows the cumulative value of all the ISL link speeds.

  For example, two ISL ports operating at 4 Gbps should show a speed of 8 Gbps.

- `Trunk vsans (admin allowed and active)` shows all the allowed VSANs.
- `Trunk vsans (up)` shows all the allowed VSANs.
- The member list shows all the ISL ports that were added to the port-channel.
- The port VSAN number should be the same as the VSAN that contains the ISLs (usually native vsan 1).

```
FC_switch_A_1(config-if)# show int port-channel 1
port-channel 1 is trunking
    Hardware is Fibre Channel
    Port WWN is 24:01:54:7f:ee:e2:8d:a0
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Speed is 8 Gbps
    Trunk vsans (admin allowed and active) (1,10,20)
    Trunk vsans (up)                       (1,10,20)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 1154832 bits/sec,144354 bytes/sec, 170
frames/sec
    5 minutes output rate 1299152 bits/sec,162394 bytes/sec, 183
frames/sec
      535724861 frames input,1069616011292 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      572290295 frames output,1144869385204 bytes
        0 discards,0 errors
      5 input OLS,11  LRR,2 NOS,0 loop inits
      14 output OLS,5 LRR, 0 NOS, 0 loop inits
    Member[1] : fc1/36
    Member[2] : fc1/40
    Interface last changed at Thu Oct 16 11:48:00 2014
```

1. Exit interface configuration on both switches:

```
end
```

2. Copy the updated configuration to the startup configuration on both fabrics:

```
copy running-config startup-config
```

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

3. Repeat the previous steps on the second switch fabric.

Related information

You need to verify that you are using the specified port assignments when you cable the FC switches when using ONTAP 9.1 and later. Refer to Port assignments for FC switches when using ONTAP 9.1 and later

Configuring FCIP ports for a single ISL on Cisco 9250i FC switches

You must configure the FCIP switch ports that connect the ISL (E-ports) by creating FCIP profiles and interfaces, and then assigning them to the IPStorage1/1 GbE interface.

About this task

This task is only for configurations using a single ISL per switch fabric, using the IPStorage1/1 interface on each switch.

This task must be performed on each FC switch.

Two FCIP profiles are created on each switch:

- Fabric 1
  - FC_switch_A_1 is configured with FCIP profiles 11 and 111.
  - FC_switch_B_1 is configured with FCIP profiles 12 and 121.
- Fabric 2
  - FC_switch_A_2 is configured with FCIP profiles 13 and 131.
  - FC_switch_B_2 is configured with FCIP profiles 14 and 141.

Steps

1. Enter configuration mode:

```
config t
```

2. Enable FCIP:

```
feature fcip
```

3. Configure the IPStorage1/1 GbE interface:

a. Enter configuration mode:

```
conf t
```

b. Specify the IPStorage1/1 interface:

```
interface IPStorage1/1
```

c. Specify the IP address and subnet mask:

```
interface ip-address subnet-mask
```

d. Specify the MTU size of 2500:

```
switchport mtu 2500
```

e. Enable the port:

```
no shutdown
```

f. Exit configuration mode:

```
exit
```

The following example shows the configuration of an IPStorage1/1 port:

```
conf t
interface IPStorage1/1
  ip address 192.168.1.201 255.255.255.0
  switchport mtu 2500
  no shutdown
exit
```

4. Configure the FCIP profile for FC-VI traffic:

a. Configure an FCIP profile and enter FCIP profile configuration mode:

```
fcip profile FCIP-profile-name
```

The profile name depends on which switch is being configured.

b. Assign the IP address of the IPStorage1/1 interface to the FCIP profile:

```
ip address ip-address
```

c. Assign the FCIP profile to TCP port 3227:

```
port 3227
```

d. Set the TCP settings:

```
tcp keepalive-timeout 1
```

```
tcp max-retransmissions 3
```

```
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3
```

```
tcp min-retransmit-time 200
```

```
tcp keepalive-timeout 1
```

```
tcp pmtu-enable reset-timeout 3600
```

```
tcp sack-enable``no tcp cwm
```

The following example shows the configuration of the FCIP profile:

```
conf t
fcip profile 11
  ip address 192.168.1.333
  port 3227
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

5. Configure the FCIP profile for storage traffic:

   a. Configure an FCIP profile with the name 111 and enter FCIP profile configuration mode:

   ```
   fcip profile 111
   ```

   b. Assign the IP address of the IPStorage1/1 interface to the FCIP profile:

   ```
   ip address ip-address
   ```

   c. Assign the FCIP profile to TCP port 3229:

   ```
   port 3229
   ```

   d. Set the TCP settings:

   ```
   tcp keepalive-timeout 1
   ```

   ```
   tcp max-retransmissions 3
   ```

```
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
3
```

```
tcp min-retransmit-time 200
```

```
tcp keepalive-timeout 1
```

```
tcp pmtu-enable reset-timeout 3600
```

```
tcp sack-enable``no tcp cwm
```

The following example shows the configuration of the FCIP profile:

```
conf t
fcip profile 111
  ip address 192.168.1.334
  port 3229
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-
time-ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm
```

6. Create the first of two FCIP interfaces:

   ```
   interface fcip 1
   ```

   This interface is used for FC-IV traffic.

   a. Select the profile 11 created previously:

      ```
      use-profile 11
      ```

   b. Set the IP address and port of the IPStorage1/1 port on the partner switch:

      peer-info ipaddr *partner-switch-port-ip* port 3227

   c. Select TCP connection 2:

      ```
      tcp-connection 2
      ```

   d. Disable compression:

      ```
      no ip-compression
      ```

e. Enable the interface:

```
no shutdown
```

f. Configure the control TCP connection to 48 and the data connection to 26to mark all packets on that differentiated services code point (DSCP) value:

```
qos control 48 data 26
```

g. Exit the interface configuration mode:

```
exit
```

The following example shows the configuration of the FCIP interface:

```
interface fcip  1
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
 peer-info ipaddr 192.168.32.334   port 3227
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

7. Create the second of two FCIP interfaces:

```
interface fcip 2
```

This interface is used for storage traffic.

a. Select the profile 111 created previously:

```
use-profile 111
```

b. Set the IP address and port of the IPStorage1/1 port on the partner switch:

```
peer-info ipaddr partner-switch-port-ip port 3229
```

c. Select TCP connection 2:

```
tcp-connection 5
```

d. Disable compression:

```
no ip-compression
```

e. Enable the interface:

```
no shutdown
```

f. Configure the control TCP connection to 48 and data connection to 26to mark all packets on that differentiated services code point (DSCP) value:

```
qos control 48 data 26
```

g. Exit the interface configuration mode:

```
exit
```

The following example shows the configuration of the FCIP interface:

```
interface fcip  2
  use-profile 11
# the port # listed in this command is the port that the remote switch
is listening on
 peer-info ipaddr 192.168.32.33e  port 3229
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

8. Configure the switchport settings on the fcip 1 interface:

a. Enter configuration mode:

```
config t
```

b. Specify the port you are configuring:

```
interface fcip 1
```

c. Shut down the port:

```
shutdown
```

d. Set the port to E mode:

```
switchport mode E
```

e. Enable the trunk mode for the port:

```
switchport trunk mode on
```

f. Set the trunk allowed vsan to 10:

```
switchport trunk allowed vsan 10
```

g. Set the speed for the port:

```
switchport speed speed-value
```

9. Configure the switchport settings on the fcip 2 interface:
   a. Enter configuration mode:

      ```
      config t
      ```

   b. Specify the port you are configuring:

      ```
      interface fcip 2
      ```

   c. Shut down the port:

      ```
      shutdown
      ```

   d. Set the port to E mode:

      ```
      switchport mode E
      ```

   e. Enable the trunk mode for the port:

      ```
      switchport trunk mode on
      ```

   f. Set the trunk allowed vsan to 20:

      ```
      switchport trunk allowed vsan 20
      ```

   g. Set the speed for the port:

      ```
      switchport speed speed-value
      ```

10. Repeat the previous steps on the second switch.

    The only differences are the appropriate IP addresses and unique FCIP profile names.

    - When configuring the first switch fabric, FC_switch_B_1 is configured with FCIP profiles 12 and 121.
    - When configuring the first switch fabric, FC_switch_A_2 is configured with FCIP profiles 13 and 131 and FC_switch_B_2 is configured with FCIP profiles 14 and 141.

11. Restart the ports on both switches:

    ```
    no shutdown
    ```

12. Exit the interface configuration on both switches:

    ```
    end
    ```

13. Copy the updated configuration to the startup configuration on both switches:

    ```
    copy running-config startup-config
    ```

```
FC_switch_A_1(config-if)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1(config-if)# end
FC_switch_B_1# copy running-config startup-config
```

14. Repeat the previous steps on the second switch fabric.

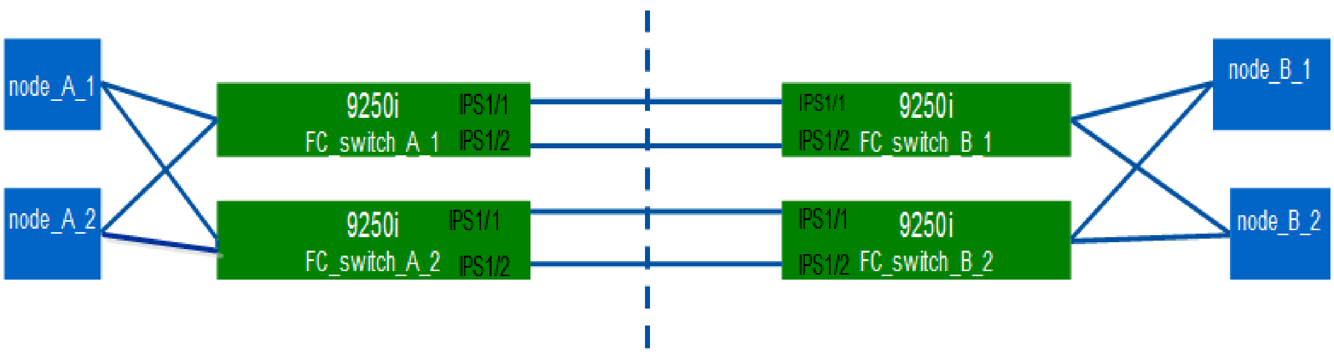
Configuring FCIP ports for a dual ISL on Cisco 9250i FC switches

You must configure the FCIP switch ports that connect the ISL (E-ports) by creating FCIP profiles and interfaces, and then assigning them to the IPStorage1/1 and IPStorage1/2 GbE interfaces.

About this task

This task is only for configurations that use a dual ISL per switch fabric, using the IPStorage1/1 and IPStorage1/2 GbE interfaces on each switch.

This task must be performed on each FC switch.



The task and examples use the following profile configuration tables:

- Fabric 1 profile configuration table
- Fabric 2 profile configuration table

Fabric 1 profile configuration table

Switch fabric	IPStorage interface	IP Address	Port type	FCIP interface	FCIP profile	Port	Peer IP/port	VSAN ID

FC_switch_A_1	IPStorage 1/1	a.a.a.a	FC-VI	fcip 1	15	3220	c.c.c.c/3230	10
			Storage	fcip 2	20	3221	c.c.c.c/3231	20
	IPStorage 1/2	b.b.b.b	FC-VI	fcip 3	25	3222	d.d.d.d/3232	10
			Storage	fcip 4	30	3223	d.d.d.d/3233	20
FC_switch_B_1	IPStorage 1/1	c.c.c.c	FC-VI	fcip 1	15	3230	a.a.a.a/3220	10
			Storage	fcip 2	20	3231	a.a.a.a/3221	20
	IPStorage 1/2	d.d.d.d	FC-VI	fcip 3	25	3232	b.b.b.b/3222	10
			Storage	fcip 4	30	3233	b.b.b.b/3223	20

Fabric 2 profile configuration table

Switch fabric	IPStorage interface	IP Address	Port type	FCIP interface	FCIP profile	Port	Peer IP/port	VSAN ID
FC_switch_A_2	IPStorage 1/1	e.e.e.e	FC-VI	fcip 1	15	3220	g.g.g.g/3230	10
			Storage	fcip 2	20	3221	g.g.g.g/3231	20
	IPStorage 1/2	f.f.f.f	FC-VI	fcip 3	25	3222	h.h.h.h/3232	10
			Storage	fcip 4	30	3223	h.h.h.h/3233	20

FC_switch_B_2	IPStorage 1/1	g.g.g.g	FC-VI	fcip 1	15	3230	e.e.e.e/3220	10
			Storage	fcip 2	20	3231	e.e.e.e/3221	20
	IPStorage 1/2	h.h.h.h	FC-VI	fcip 3	25	3232	f.f.f.f/3222	10
			Storage	fcip 4	30	3233	f.f.f.f/3223	20

Steps

1. Enter configuration mode:

   ```
   config t
   ```

2. Enable FCIP:

   ```
   feature fcip
   ```

3. On each switch, configure the two IPStorage interfaces (IPStorage1/1 and IPStorage1/2):

   a. Enter configuration mode:

   ```
   conf t
   ```

   b. Specify the IPStorage interface to create:

   ```
   interface ipstorage
   ```

   The *ipstorage* parameter value is "IPStorage1/1" or "IPStorage1/2".

   c. Specify the IP address and subnet mask of the IPStorage interface previously specified:

   ```
   interface ip-address subnet-mask
   ```

   > On each switch, the IPStorage interfaces "IPStorage1/1" and "IPStorage1/2" must have different IP addresses.

   d. Specify the MTU size as 2500:

   ```
   switchport mtu 2500
   ```

   e. Enable the port:

   ```
   no shutdown
   ```

   f. Exit configuration mode:

   ```
   exit
   ```

   g. Repeat Substep "a" through Substep "f" to configure the IPStorage1/2 GbE interface with a different IP address.

4. Configure the FCIP profiles for FC-VI and storage traffic with the profile names given in the profile configuration table:

   a. Enter configuration mode:

      ```
      conf t
      ```

   b. Configure the FCIP profiles with the following profile names:

      ```
      fcip profile FCIP-profile-name
      ```

      The following list provides the values for the `FCIP-profile-name` parameter:

      - 15 for FC-VI on IPStorage1/1
      - 20 for storage on IPStorage1/1
      - 25 for FC-VI on IPStorage1/2
      - 30 for storage on IPStorage1/2

   c. Assign the FCIP profile ports according to the profile configuration table:

      ```
      port port_number
      ```

   d. Set the TCP settings:

      ```
      tcp keepalive-timeout 1

      tcp max-retransmissions 3

      max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-ms
      3

      tcp min-retransmit-time 200

      tcp keepalive-timeout 1

      tcp pmtu-enable reset-timeout 3600

      tcp sack-enable

      no tcp cwm
      ```

5. Create FCIP interfaces:

   ```
   interface fcip FCIP_interface
   ```

   The `FCIP_interface` parameter value is "1", "2", "3", or "4" as shown in the profile configuration table.

   a. Map interfaces to the previously created profiles:

      ```
      use-profile profile
      ```

   b. Set the peer IP address and peer profile port number:

```
peer-info peer IPstorage ipaddr port peer_profile_port_number
```

c. Select the TCP connections:

```
tcp-connection connection-#
```

The `connection-#` parameter value is "2" for FC-VI profiles and "5" for storage profiles.

d. Disable compression:

```
no ip-compression
```

e. Enable the interface:

```
no shutdown
```

f. Configure the control TCP connection to 48 and the data connection to 26to mark all packets that have differentiated services code point (DSCP) value:

```
qos control 48 data 26
```

g. Exit configuration mode:

```
exit
```

6. Configure the switchport settings on each FCIP interface:

a. Enter configuration mode:

```
config t
```

b. Specify the port that you are configuring:

```
interface fcip 1
```

c. Shut down the port:

```
shutdown
```

d. Set the port to E mode:

```
switchport mode E
```

e. Enable the trunk mode for the port:

```
switchport trunk mode on
```

f. Specify the trunk that is allowed on a specific VSAN:

```
switchport trunk allowed vsan vsan_id
```

The *vsan_id* parameter value is "VSAN 10" for FC-VI profiles and "VSAN 20" for storage profiles.

g. Set the speed for the port:

```
switchport speed speed-value
```

h. Exit configuration mode:

```
exit
```

7. Copy the updated configuration to the startup configuration on both switches:

```
copy running-config startup-config
```

The following examples show the configuration of FCIP ports for a dual ISL in fabric 1 switches FC_switch_A_1 and FC_switch_B_1.

For FC_switch_A_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# no in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings

feature  fcip

conf t
interface IPStorage1/1
#  IP address:  a.a.a.a
#  Mask:  y.y.y.y
  ip address <a.a.a.a   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit
conf t
fcip profile 15
  ip address <a.a.a.a>
  port 3220
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
```

```
  ip address <a.a.a.a>
  port 3221
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
#  IP address:  b.b.b.b
#  Mask:  y.y.y.y
  ip address <b.b.b.b   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 25
  ip address <b.b.b.b>
  port 3222
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <b.b.b.b>
  port 3223
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
```

```
  tcp sack-enable
  no tcp cwm
interface fcip  1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <c.c.c.c>  port 3230
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <c.c.c.c>  port 3231
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < d.d.d.d >  port 3232
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < d.d.d.d >  port 3233
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit
```

```
conf t
interface fcip  1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit

conf t
interface fcip  3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

For FC_switch_B_1:

```
FC_switch_A_1# config t
FC_switch_A_1(config)# in-order-guarantee vsan 10
FC_switch_A_1(config-vsan-db)# end
FC_switch_A_1# copy running-config startup-config

# fcip settings
```

```
feature  fcip

conf t
interface IPStorage1/1
#  IP address:  c.c.c.c
#  Mask:  y.y.y.y
  ip address <c.c.c.c   y.y.y.y>
  switchport mtu 2500
  no shutdown
exit

conf t
fcip profile 15
  ip address <c.c.c.c>
  port 3230
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 20
  ip address <c.c.c.c>
  port 3231
  tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
interface IPStorage1/2
#  IP address:  d.d.d.d
#  Mask:  y.y.y.y
  ip address <b.b.b.b   y.y.y.y>
  switchport mtu 2500
  no shutdown
```

```
exit

conf t
fcip profile 25
  ip address <d.d.d.d>
  port 3232
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

conf t
fcip profile 30
  ip address <d.d.d.d>
  port 3233
tcp keepalive-timeout 1
tcp max-retransmissions 3
max-bandwidth-mbps 5000 min-available-bandwidth-mbps 4500 round-trip-time-
ms 3
  tcp min-retransmit-time 200
  tcp keepalive-timeout 1
  tcp pmtu-enable reset-timeout 3600
  tcp sack-enable
  no tcp cwm

interface fcip  1
  use-profile 15
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <a.a.a.a>  port 3220
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  2
  use-profile 20
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr <a.a.a.a>  port 3221
```

```
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  3
  use-profile 25
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < b.b.b.b >  port 3222
  tcp-connection 2
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

interface fcip  4
  use-profile 30
# the port # listed in this command is the port that the remote switch is
listening on
 peer-info ipaddr < b.b.b.b >  port 3223
  tcp-connection 5
  no ip-compression
  no shutdown
  qos control 48 data 26
exit

conf t
interface fcip  1
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  2
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

```
conf t
interface fcip  3
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 10
no shutdown
exit

conf t
interface fcip  4
shutdown
switchport mode E
switchport trunk mode on
switchport trunk allowed vsan 20
no shutdown
exit
```

Configuring zoning on a Cisco FC switch

You must assign the switch ports to separate zones to isolate storage (HBA) and controller (FC-VI) traffic.

About this task

These steps must be performed on both FC switch fabrics.

The following steps use the zoning described in the section Zoning for a FibreBridge 7500N in a four-node MetroCluster configuration. Refer to Zoning for FC-VI ports.

Steps

1. Clear the existing zones and zone set, if present.

   a. Determine which zones and zone sets are active:

      `show zoneset active`

      ```
      FC_switch_A_1# show zoneset active

      FC_switch_B_1# show zoneset active
      ```

   b. Disable the active zone sets identified in the previous step:

      `no zoneset activate name` *`zoneset_name`* `vsan` *`vsan_id`*

      The following example shows two zone sets being disabled:

      ▪ ZoneSet_A on FC_switch_A_1 in VSAN 10

▪ ZoneSet_B on FC_switch_B_1 in VSAN 20

```
FC_switch_A_1# no zoneset activate name ZoneSet_A vsan 10

FC_switch_B_1# no zoneset activate name ZoneSet_B vsan 20
```

a. After all zone sets are deactivated, clear the zone database:

   `clear zone database` *`zone-name`*

```
FC_switch_A_1# clear zone database 10
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# clear zone database 20
FC_switch_B_1# copy running-config startup-config
```

2. Obtain the switch worldwide name (WWN):

   `show wwn switch`

3. Configure the basic zone settings:

   a. Set the default zoning policy to "permit":

      `no system default zone default-zone permit`

   b. Enable the full zone distribution:

      `system default zone distribute full`

   c. Set the default zoning policy for each VSAN:

      `no zone default-zone permit` *`vsanid`*

   d. Set the default full zone distribution for each VSAN:

      `zoneset distribute full` *`vsanid`*

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# no system default zone default-zone permit
FC_switch_A_1(config)# system default zone distribute full
FC_switch_A_1(config)# no zone default-zone permit 10
FC_switch_A_1(config)# no zone default-zone permit 20
FC_switch_A_1(config)# zoneset distribute full vsan 10
FC_switch_A_1(config)# zoneset distribute full vsan 20
FC_switch_A_1(config)# end
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# conf t
FC_switch_B_1(config)# no system default zone default-zone permit
FC_switch_B_1(config)# system default zone distribute full
FC_switch_B_1(config)# no zone default-zone permit 10
FC_switch_B_1(config)# no zone default-zone permit 20
FC_switch_B_1(config)# zoneset distribute full vsan 10
FC_switch_B_1(config)# zoneset distribute full vsan 20
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
```

4. Create storage zones and add the storage ports to them.

   > Perform these steps on only one switch in each fabric.

   The zoning depends on the model FC-to-SAS bridge you are using. For details, see the section for your model bridge. The examples show Brocade switch ports, so adjust your ports accordingly.

   - Zoning for FibreBridge 6500N bridges, or FibreBridge 7500N, or 7600N bridges using one FC port
   - Zoning for FibreBridge 7500N bridges using both FC ports

   Each storage zone contains the HBA initiator ports from all controllers and one single port connecting an FC-to-SAS bridge.

   a. Create the storage zones:

      `zone name` *`STOR-zone-name`* `vsan` *`vsanid`*

   b. Add storage ports to the zone:

      `member portswitch WWN`

   c. Activate the zone set:

      `zoneset activate name` *`STOR-zone-name-setname`* `vsan` *`vsan-id`*

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name STOR_Zone_1_20_25 vsan 20
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/5 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/9 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/17 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/21 swwn
20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/25 swwn
20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

5. Create a storage zone set and add the storage zones to the new set.

   Perform these steps on only one switch in the fabric.

   a. Create the storage zone set:

      `zoneset name STOR-zone-set-name vsan vsan-id`

   b. Add storage zones to the zone set:

      `member STOR-zone-name`

   c. Activate the zone set:

      `zoneset activate name STOR-zone-set-name vsan vsanid`

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name STORI_Zoneset_1_20 vsan 20
FC_switch_A_1(config-zoneset)# member STOR_Zone_1_20_25
...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name STOR_ZoneSet_1_20 vsan
20
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

6. Create FCVI zones and add the FCVI ports to them.

   Each FCVI zone contains the FCVI ports from all the controllers of one DR Group.

   > Perform these steps on only one switch in the fabric.

   The zoning depends on the model FC-to-SAS bridge you are using. For details, see the section for your model bridge. The examples show Brocade switch ports, so adjust your ports accordingly.

   - Zoning for FibreBridge 6500N bridges, or FibreBridge 7500N, or 7600N bridges using one FC port
   - Zoning for FibreBridge 7500N bridges using both FC ports

   Each storage zone contains the HBA initiator ports from all controllers and one single port connecting an FC-to-SAS bridge.

   a. Create the FCVI zones:

      `zone name` *`FCVI-zone-name`* `vsan` *`vsanid`*

   b. Add FCVI ports to the zone:

      `member` *`FCVI-zone-name`*

   c. Activate the zone set:

      `zoneset activate name` *`FCVI-zone-name-set-name`* `vsan` *`vsanid`*

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zone name FCVI_Zone_1_10_25 vsan 10
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:cb:78
FC_switch_A_1(config-zone)# member interface fc1/1
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# member interface fc1/2
swwn20:00:00:05:9b:24:12:99
FC_switch_A_1(config-zone)# end
FC_switch_A_1# copy running-config startup-config
```

7. Create an FCVI zone set and add the FCVI zones to it:

   Perform these steps on only one switch in the fabric.

   a. Create the FCVI zone set:

      `zoneset name` *`FCVI_zone_set_name`* `vsan` *`vsan-id`*

   b. Add FCVI zones to the zone set:

      `member` *`FCVI_zonename`*

   c. Activate the zone set:

      `zoneset activate name` *`FCVI_zone_set_name`* `vsan` *`vsan-id`*

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# zoneset name FCVI_Zoneset_1_10 vsan 10
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_25
FC_switch_A_1(config-zoneset)# member FCVI_Zone_1_10_29
    ...
FC_switch_A_1(config-zoneset)# exit
FC_switch_A_1(config)# zoneset activate name FCVI_ZoneSet_1_10 vsan 10
FC_switch_A_1(config)# exit
FC_switch_A_1# copy running-config startup-config
```

8. Verify the zoning:

   `show zone`

9. Repeat the previous steps on the second FC switch fabric.

Ensuring the FC switch configuration is saved

You must make sure the FC switch configuration is saved to the startup config on all switches.

Step

Issue the following command on both FC switch fabrics:

`copy running-config startup-config`

```
FC_switch_A_1# copy running-config startup-config

FC_switch_B_1# copy running-config startup-config
```

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

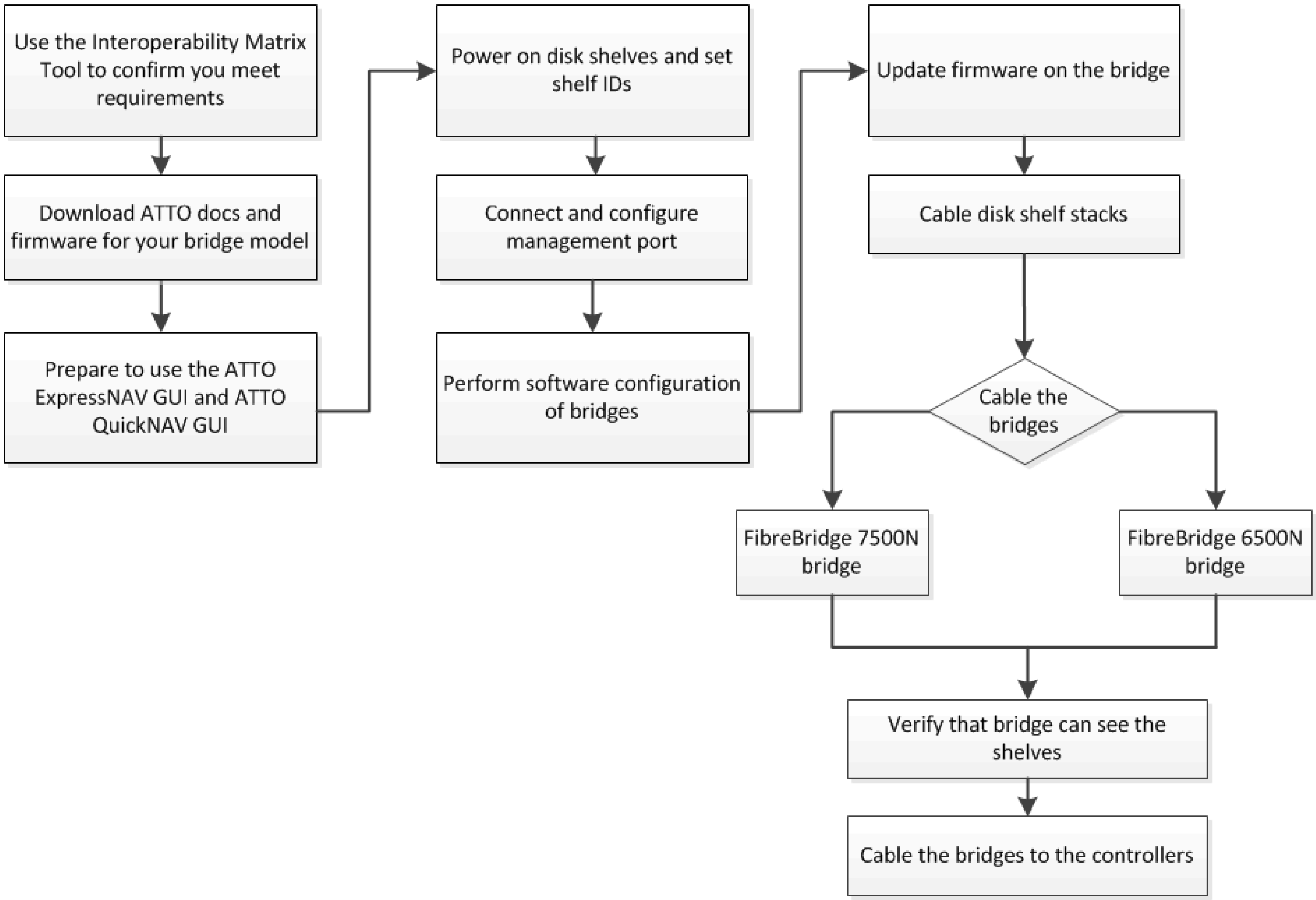
For systems received from the factory, the FC-to-SAS bridges are preconfigured and do not require additional configuration.

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:



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. Beginning with ONTAP 9.8, out-of-band management is deprecated.

> Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

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.

The availability of in-band management of the bridges depends on the version of ONTAP:

- Starting with ONTAP 9.8, bridges are managed via in-band connections by default and out-of-band management of the bridges via SNMP is deprecated.
- ONTAP 9.5 through 9.7: Either in-band management or out-of-band SNMP management is supported.
- Prior to ONTAP 9.5, only out-of-band SNMP management is supported.

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.

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.

  In the NetApp Interoperability Matrix Tool (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.

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

   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.

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.

  > 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 IOM3 modules is not supported within the same storage stack. A mix of IOM12 modules and IOM6 modules is supported within the same storage stack if your system is running a supported version of ONTAP.

> 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

> SAS shelves in MetroCluster configurations do not support ACP cabling.

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.

Starting with ONTAP 9.8, *in-band management* of the bridges is supported by default and out-of-band SNMP management is deprecated.

This task is required if you are **not** using in-band management to manage the bridges. In this case, 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 a service, if desired, by issuing the `set closeport` command and repeating the command as necessary until all desired services are disabled:

   ```
   set closeport service
   ```

   The `set closeport` command disables a single service at a time.

   The parameter *`service`* can be specified as 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.

4. If you are enabling SNMP, you must also issue following command:

   ```
   set SNMP enabled
   ```

   SNMP is the only protocol that requires a separate enable command.

5. Save the configuration:

   ```
   saveconfiguration
   ```

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.

> Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

   The Ethernet management 1 port enables you to quickly download the bridge firmware (using ATTO ExpressNAV 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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

   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.

   > 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 the Ethernet port. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

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

   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

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

   `set bridgename` *`bridge_name`*

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

   `set SNMP enabled`

   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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

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.

> The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the FC port of the controller module to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

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.

> The FCConnMode setting is not required when configuring a FibreBridge 7600N bridge.

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`*

    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`*

> SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used.

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:

```
SASPortDisable b

SAS Port B has been disabled.
```

6. Secure access to the bridge and save the bridge's configuration. Choose an option from below depending on the version of ONTAP your system is running.

ONTAP version	Steps
ONTAP 9.5 or later	a. View the status of the bridges: `storage bridge show` The output shows which bridge is not secured. b. Secure the bridge: `securebridge`

ONTAP 9.4 or earlier	a. View the status of the bridges:
	
	`storage bridge show`
	
	The output shows which bridge is not secured.
	
	b. Check the status of the unsecured bridge's ports:
	
	`info`
	
	The output shows the status of Ethernet ports MP1 and MP2.
	
	c. If Ethernet port MP1 is enabled, run:
	
	`set EthernetPort mp1 disabled`
	
	If Ethernet port MP2 is also enabled, repeat the previous substep for port MP2.
	
	d. Save the bridge's configuration.
	
	You must run the following commands:
	
	`SaveConfiguration`
	
	`FirmwareRestart`
	
	You are prompted to restart the bridge.

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.

   Maintain MetroCluster Components

Related information

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

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
- Cabling a FibreBridge 7600N or 7500N bridge with disk shelves using IOM6 or IOM3 modules
- Cabling a FibreBridge 6500N bridge with disk shelves using IOM6 or IOM3 modules

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).

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.

Steps

1. 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 each MetroCluster DR group (including both sites).
2. Cable disk shelves to the FibreBridge bridges.

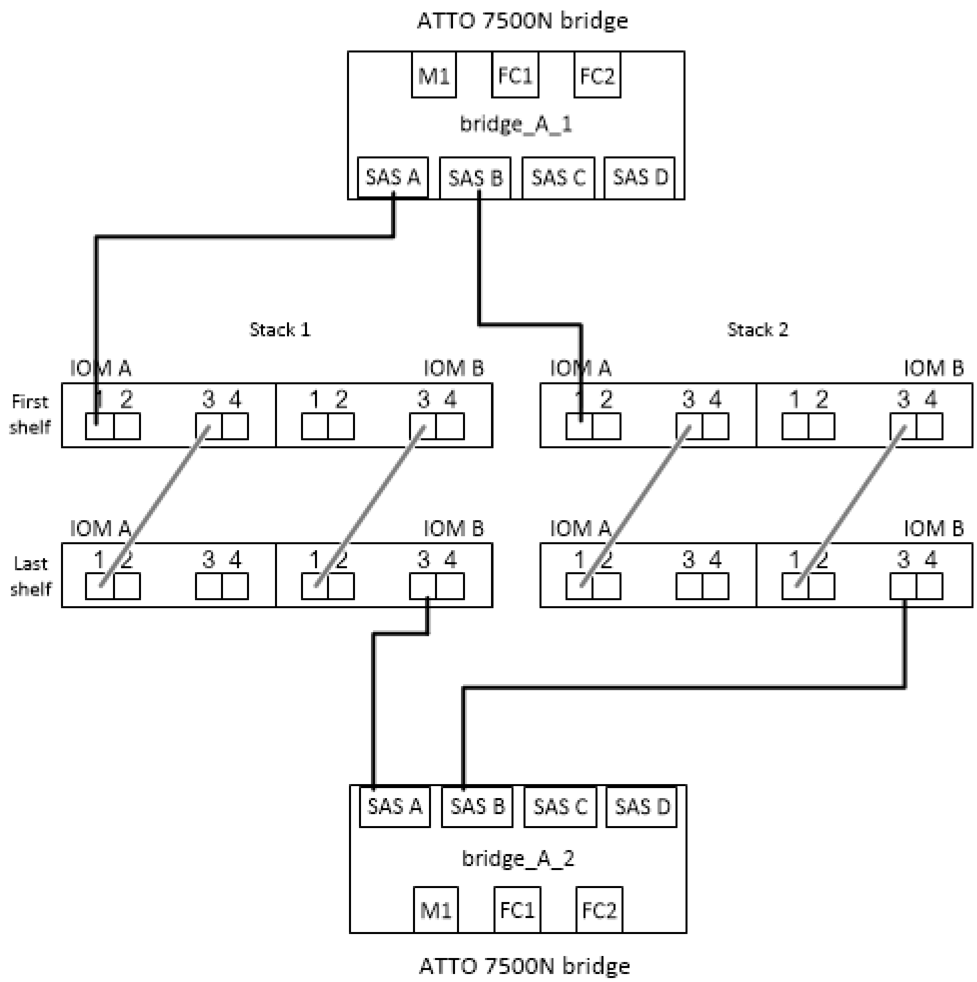
    a. For the first stack of disk shelves, cable IOM A of the first shelf to SAS port A on FibreBridge A, and cable IOM B of the last shelf to SAS port A on FibreBridge B.

    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.

    > 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.

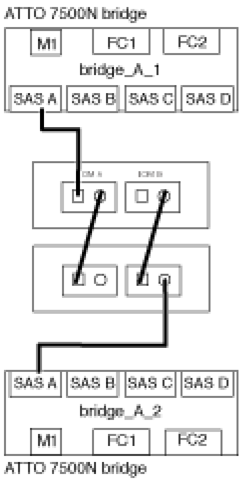
    a. For the first stack of shelves, cable IOM A square port of the first shelf to SAS port A on FibreBridge A.

    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.

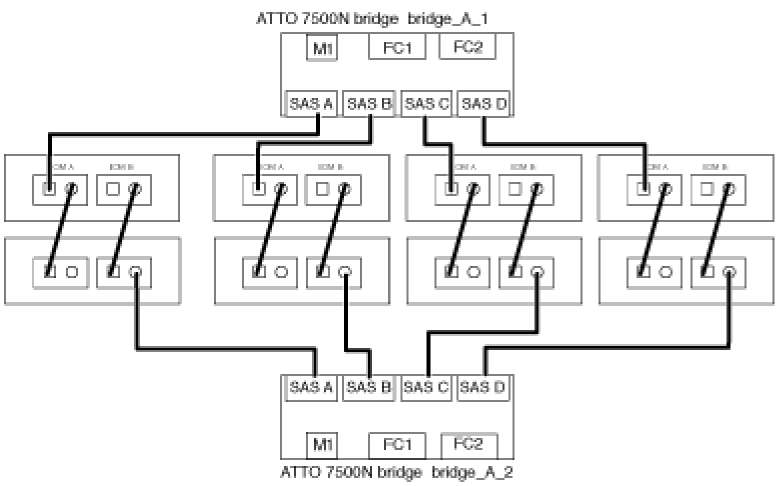
    [SAS Disk Shelves Installation and Service Guide for DS4243, DS2246, DS4486, and DS4246](#)

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.

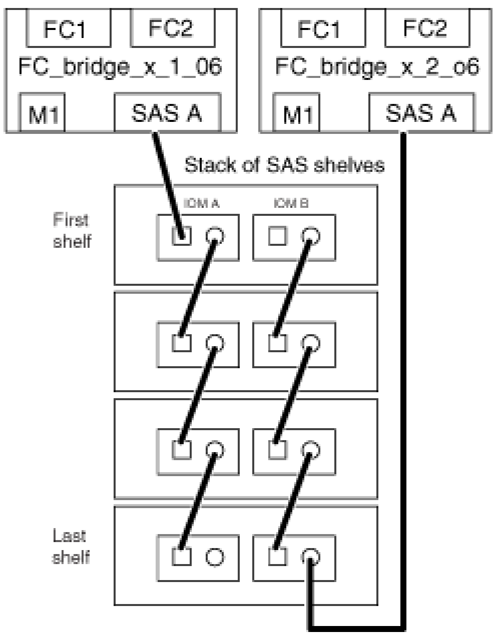
   For information about daisy-chaining disk shelves, see the *Installation and Service Guide* for your disk shelf model.

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.

   > The SAS port B bridge is disabled.

   The following illustration shows a set of bridges cabled to a stack of four disk shelves:



Verifying bridge connectivity and cabling the bridge FC ports

You should verify that each bridge can detect all of the disk drives, and then cable each bridge to the local FC switches.

Steps

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

If you are using the…	Then…

ATTO ExpressNAV GUI	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. 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. c. Click **Advanced**. d. View the connected devices by using the sastargets command, and then click **Submit**.
Serial port connection	View the connected devices: `sastargets`

The 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. For example, the following output shows that 10 disks are connected:

+

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

+ NOTE: If the text "response truncated" appears at the beginning of the output, you can use Telnet to connect to the bridge and enter the same command to see all of the output.

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

If the output is…	**Then…**

Correct	Repeat Step 1 for each remaining bridge.
Not correct	a. Check for loose SAS cables or correct the SAS cabling by repeating the cabling. Cabling disk shelves to the bridges b. Repeat Step 1.

2. Cable each bridge to the local FC switches, using the cabling in the table for your configuration and switch model and FC-to-SAS bridge model:

> The second FC port connection on the FibreBridge 7500N bridge should not be cabled until zoning has been completed.

See the port assignments for your version of ONTAP.

3. Repeat the previous step on the bridges at the partner site.

Related information

Port assignments for FC switches when using ONTAP 9.1 and later

You need to verify that you are using the specified port assignments when you cable the FC switches when using ONTAP 9.1 and later.

Port assignments for FC switches when using ONTAP 9.0

You need to verify that you are using the specified port assignments when you cable the FC switches. The port assignments are different between ONTAP 9.0 and later version of ONTAP.

Securing or unsecuring the FibreBridge bridge

To easily disable potentially unsecure Ethernet protocols on a bridge, beginning with ONTAP 9.5 you can secure the bridge. This disables the bridge's Ethernet ports. You can also reenable Ethernet access.

About this task

- Securing the bridge disables telnet and other IP port protocols and services (FTP, ExpressNAV, ICMP, or QuickNAV) on the bridge.
- This procedure uses out-of-band management using the ONTAP prompt, which is available beginning with ONTAP 9.5.

  You can issue the commands from the bridge CLI if you are not using out-of-band management.
- The `unsecurebridge` command can be used to reenable the Ethernet ports.
- In ONTAP 9.7 and earlier, running the `securebridge` command on the ATTO FibreBridge might not update the bridge status correctly on the partner cluster. If this occurs, run the `securebridge` command from the partner cluster.

Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

Steps

1. From the ONTAP prompt of the cluster containing the bridge, secure or unsecure the bridge.
   - The following command secures bridge_A_1:

     ```
     cluster_A> storage bridge run-cli -bridge bridge_A_1 -command securebridge
     ```

   - The following command unsecures bridge_A_1:

     ```
     cluster_A> storage bridge run-cli -bridge bridge_A_1 -command unsecurebridge
     ```

2. From the ONTAP prompt of the cluster containing the bridge, save the bridge configuration:

   `storage bridge run-cli -bridge` *`bridge-name`* `-command saveconfiguration`

   The following command secures bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   saveconfiguration
   ```

3. From the ONTAP prompt of the cluster containing the bridge, restart the bridge's firmware:

   `storage bridge run-cli -bridge` *`bridge-name`* `-command firmwarerestart`

   The following command secures bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command firmwarerestart
   ```

Configuring hardware for sharing a Brocade 6510 FC fabric during transition

If your 7-Mode fabric MetroCluster configuration uses Brocade 6510 switches, you can share the existing switch fabrics with the new clustered MetroCluster configuration. Shared switch fabrics means the new MetroCluster configuration does not require a new, separate switch fabric. This temporary configuration is only supported with the Brocade 6510 switch for transition purposes.

Before you begin

- The 7-Mode fabric MetroCluster must be using Brocade 6510 switches.

  If the MetroCluster configuration is currently not using Brocade 6510 switches, the switches must be upgraded to Brocade 6510 prior to using this procedure.

- The 7-Mode fabric MetroCluster configuration must be using SAS storage shelves only.

  If the existing configuration includes FC storage shelves (such as the DS14mk4 FC), FC switch fabric sharing is not supported.

- The SFPs on the switch ports used by the new, clustered MetroCluster configuration must support 16-Gbps rates.

  The existing 7-Mode fabric MetroCluster can remain connected to ports using 8-Gbps or 16-Gbps SFPs.

- On each of the four Brocade 6510 switches, ports 24 through 45 must be available to connect the ports of the new MetroCluster components.
- You should verify that the existing Inter-Switch Links (ISLs) are on ports 46 and 47.
- The Brocade 6510 switches must be running a FOS firmware version that is supported on both the 7-Mode fabric MetroCluster and clustered ONTAP MetroCluster configuration.

After you finish

After sharing the fabric and completing the MetroCluster configuration, you can transition data from the 7-Mode fabric MetroCluster configuration.

After transitioning the data, you can remove the 7-Mode fabric MetroCluster cabling and, if desired, move the clustered ONTAP MetroCluster cabling to the lower-numbered ports previously used for the 7-Mode MetroCluster cabling. The ports are shown in the section "Reviewing FC switch port assignments for a four node MetroCluster." You must adjust the zoning for the rearranged ports.

Port assignments for FC switches when using ONTAP 9.1 and later

Related information

Copy-based transition

Reviewing Brocade license requirements

You need certain licenses for the switches in a MetroCluster configuration. You must install these licenses on all four switches.

The MetroCluster configuration has the following Brocade license requirements:

- Trunking license for systems using more than one ISL, as recommended.
- Extended Fabric license (for ISL distances over 6 km)
- Enterprise license for sites with more than one ISL and an ISL distance greater than 6 km

  The Enterprise license includes Brocade Network Advisor and all licenses except for additional port licenses.

You can verify that the licenses are installed by using the `licenseshow` command. If you do not have these licenses, you should contact your sales representative before proceeding.

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 controller modules, the switch types, and the number of disk shelf stacks in your configuration.

2. Properly ground yourself.
3. Install the controller modules in the rack or cabinet.

   AFF and FAS Documentation Center

4. Install the FC switches in the rack or cabinet.
5. Install the disk shelves, power them on, and then set the shelf IDs.
   - You must power-cycle each disk shelf.
   - Shelf IDs must be unique for each SAS disk shelf within each MetroCluster DR group (including both sites).
6. 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.

      The *ATTO FibreBridge Installation and Operation Manual* for your bridge model contains more information and an illustration of the installation.

      > For adequate port space access and FRU serviceability, you must leave 1U space below the bridge pair and cover this space with a tool-less blanking panel.

   b. Connect each bridge to a power source that provides a proper ground.
   c. Power on each bridge.

      > 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 new MetroCluster controllers to the existing FC fabrics

On each controller in the clustered ONTAP MetroCluster configuration, the FC-VI adapter and HBAs must be cabled to specific ports on the existing FC switches.

Steps

1. Cable the FC-VI and HBA ports according to the following table:

Site A		**Site B**	
Connect this Site A component and port…	**FC_switch_A_1 port…**	**Connect this Site B component and port…**	**FC_switch_B_1 port…**

controller_A_1 FC-VI port 1	32	controller_B_1 FC-VI port 1	32
controller_A_1 HBA port 1	33	controller_B_1 HBA port 1	33
controller_A_1 HBA port 2	34	controller_B_1 HBA port 2	34
controller_A_2 FC-VI port 1	35	controller_B_2 FC-VI port 1	35
controller_A_2 HBA 1	36	controller_B_2 HBA 1	36
controller_A_2 HBA 2	37	controller_B_2 HBA 2	37

2. Cable each FC-SAS bridge in the first switch fabric to the FC switches.

   The number of bridges varies depending on the number of SAS storage stacks.

Site A		**Site B**	
Cable this site A bridge…	**FC_switch_A_1 port…**	**Cable this Site B bridge…**	**FC_switch_B_1 port…**
bridge_A_1_38	38	bridge_B_1_38	38
bridge_A_1_39	39	bridge_B_1_39	39

3. Cable each bridge in the second switch fabric to the FC switches.

   The number of bridges varies depending on the number of SAS storage stacks.

Site A		**Site B**	
Cable this site A bridge…	**FC_switch_A_2 port…**	**Cable this Site B bridge…**	**FC_switch_B_2 port…**
bridge_A_2_38	38	bridge_B_2_38	38
bridge_A_2_39	39	bridge_B_2_39	39

Configuring switch fabrics sharing between the 7-Mode and clustered MetroCluster configuration

To share switch fabrics between the existing 7-Mode fabric MetroCluster and the new MetroCluster configuration, you must set up specific zoning and other settings that are different than an unshared configuration.

About this task

This task must be performed on both switch fabrics, one at a time.

Disabling one of the switch fabrics

You must disable one of the switch fabrics so you can modify its configuration. After you complete the configuration and reenable the switch fabric, you will repeat the process on the other fabric.

Before you begin

You must have run the fmc_dc utility on the existing 7-Mode fabric MetroCluster configuration and resolved any issues prior to beginning the configuration process.

About this task

To ensure continued operation of the MetroCluster configuration, you must not disable the second fabric while the first fabric is disabled.

Steps

1. Disable each of the switches in the fabric:

   `switchCfgPersistentDisable`

   If this command is not available, use the `switchDisable` command.

   - The following example shows the command issued on FC_switch_A_1:

     ```
     FC_switch_A_1:admin> switchCfgPersistentDisable
     ```

   - The following example shows the command issued on FC_switch_B_1:

     ```
     FC_switch_B_1:admin> switchCfgPersistentDisable
     ```

2. Ensure that the 7-Mode MetroCluster configuration is functioning correctly using the redundant fabric:

   a. Confirm that controller failover is healthy:
      `cf status`

      ```
      node_A> cf status
      Controller Failover enabled, node_A is up.
      VIA Interconnect is up (link 0 down, link 1 up).
      ```

   b. Confirm that disks are visible:
      `storage show disk -p`

```
node_A> storage show disk -p

PRIMARY                      PORT  SECONDARY           PORT SHELF BAY
---------------------------- ----  ------------------ ---- ---------
Brocade-6510-2K0GG:5.126L27  B                                 1    0
Brocade-6510-2K0GG:5.126L28  B                                 1    1
Brocade-6510-2K0GG:5.126L29  B                                 1    2
Brocade-6510-2K0GG:5.126L30  B                                 1    3
Brocade-6510-2K0GG:5.126L31  B                                 1    4

.
.
.
```

c. Confirm that the aggregates are healthy:
`aggr status`

```
node_A> aggr status
           Aggr State           Status              Options
          aggr0 online          raid_dp, aggr       root, nosnap=on
                                mirrored
                                64-bit
```

Deleting TI zoning and configuring IOD settings

You must delete the existing TI zoning and reconfigure in-order-delivery (IOD) settings on the switch fabric.

Steps

1. Identify the TI zones that are configured on the fabric:

   `zone --show`

   The following example shows the zone FCVI_TI_FAB_2.

```
Brocade-6510:admin> zone --show
   Defined TI zone configuration:
   TI Zone Name:   FCVI_TI_FAB_2
   Port List:      1,0; 1,3; 2,0; 2,3
   configured Status: Activated / Failover-Disabled
   Enabled Status: Activated / Failover-Disabled
```

2. Delete the TI zones:

`zone --delete *zone-name*`

The following example shows the deletion of zone FCVI_TI_FAB_2.

```
Brocade-6510:admin> zone --delete FCVI_TI_FAB_2
```

3. Confirm that the zones have been deleted:

   `zone --show`

   The output should be similar to the following:

```
Brocade-6510:admin> zone --show

    Defined TI zone configuration:
    no TI zone configuration defined
```

4. Save the configuration:

   `cfgsave`

5. Enable in-order-delivery:

   `iodset`

6. Select Advanced Performance Tuning (APT) policy 1, the Port Based Routing Policy:

   `aptpolicy 1`

7. Disable Dynamic Load Sharing (DLS):

   `dlsreset`

8. Verify the IOD settings using the following commands:

   `iodshow`

   `aptpolicy`

   `dlsshow`

   The output should be similar to the following:

```
Brocade-6510:admin> iodshow

IOD is set

Brocade-6510:admin> aptpolicy
 Current Policy: 1

 3 : Default Policy
 1: Port Based Routing Policy
 2: Device Based Routing Policy (FICON support only)
 3: Exchange Based Routing Policy
Brocade-6510:admin> dlsshow

DLS is not set
```

Ensuring ISLs are in the same port group and configuring zoning

You must make sure that the Inter-Switch Links (ISLs) are in the same port group and configure zoning for the MetroCluster configurations to successfully share the switch fabrics.

Steps

1. If the ISLs are not in the same port group, move one of the ISL ports to the same port group as the other one.

   You can use any available port except 32 through 45, which are used by the new MetroCluster configuration. The recommended ISL ports are 46 and 47.

2. Follow the steps in Configuring zoning on Brocade FC switches section to enable trunking and the QoS zone.

   The port numbers when sharing fabrics are different than those shown in the section. When sharing, use ports 46 and 47 for the ISL ports. If you moved your ISL ports, you need to use the procedure in the Configuring the E-ports (ISL ports) on a Brocade FC switch section to configure the ports.

3. Follow the steps in the Configuring the non-E ports on the Brocade switch section to configure the non-E ports.
4. Do not delete the zones or zone sets that already exist in the backend switches (for the 7-Mode fabric MetroCluster) except the Traffic Isolation (TI) zones in Step 3.
5. Follow the steps in the Configuring the E-ports (ISL ports) on a Brocade FC switch section to add the zones required by the new MetroCluster to the existing zone sets.

   The following example shows the commands and system output for creating the zones:

```
Brocade-6510-2K0GG:admin> zonecreate "QOSH2_FCVI_1", "2,32; 2,35; 1,32;
1,35"

Brocade-6510-2K0GG:admin> zonecreate "STOR_A_2_47", "2,33; 2,34; 2,36;
2,37; 1,33; 1,34; 1,36; 1,37; 1,47"

Brocade-6510-2K0GG:admin> zonecreate "STOR_B_2_47", "2,33; 2,34; 2,36;
2,37; 1,33; 1,34; 1,36; 1,37; 2,47"


Brocade-6510-2K0GG:admin> cfgadd config_1_FAB2, "QOSH2_FCVI_1;
STOR_A_2_47; STOR_B_2_47"

Brocade-6510-2K0GG:admin> cfgenable "config_1_FAB2"
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the
current configuration selected. If the update includes changes
to one or more traffic isolation zones, the update may result in
localized disruption to traffic on ports associated with
the traffic isolation zone changes
Do you want to enable 'config_1_FAB2' configuration  (yes, y, no, n):
[no] yes

Brocade-6510-2K0GG:admin> cfgsave
You are about to save the Defined zoning configuration. This
action will only save the changes on Defined configuration.
Do you want to save the Defined zoning configuration only?  (yes, y, no,
n): [no] yes
Nothing changed: nothing to save, returning ...
Brocade-6510-2K0GG:admin>
```

Reenabling the switch fabric and verifying the operation

You must enable the FC switch fabric and ensure that the switches and devices are operating correctly.

Steps

1. Enable the switches:

   ```
   switchCfgPersistentEnable
   ```

   If this command is not available, the switch should be in the enabled state after the `fastBoot` command is issued.

   ◦ The following example shows the command issued on FC_switch_A_1:

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

  - The following example shows the command issued on FC_switch_B_1:

```
FC_switch_B_1:admin> switchCfgPersistentEnable
```

2. Verify that the switches are online and all devices are properly logged in:

   `switchShow`

   The following example shows the command issued on FC_switch_A_1:

```
FC_switch_A_1:admin> switchShow
```

   The following example shows the command issued on FC_switch_B_1:

```
FC_switch_B_1:admin> switchShow
```

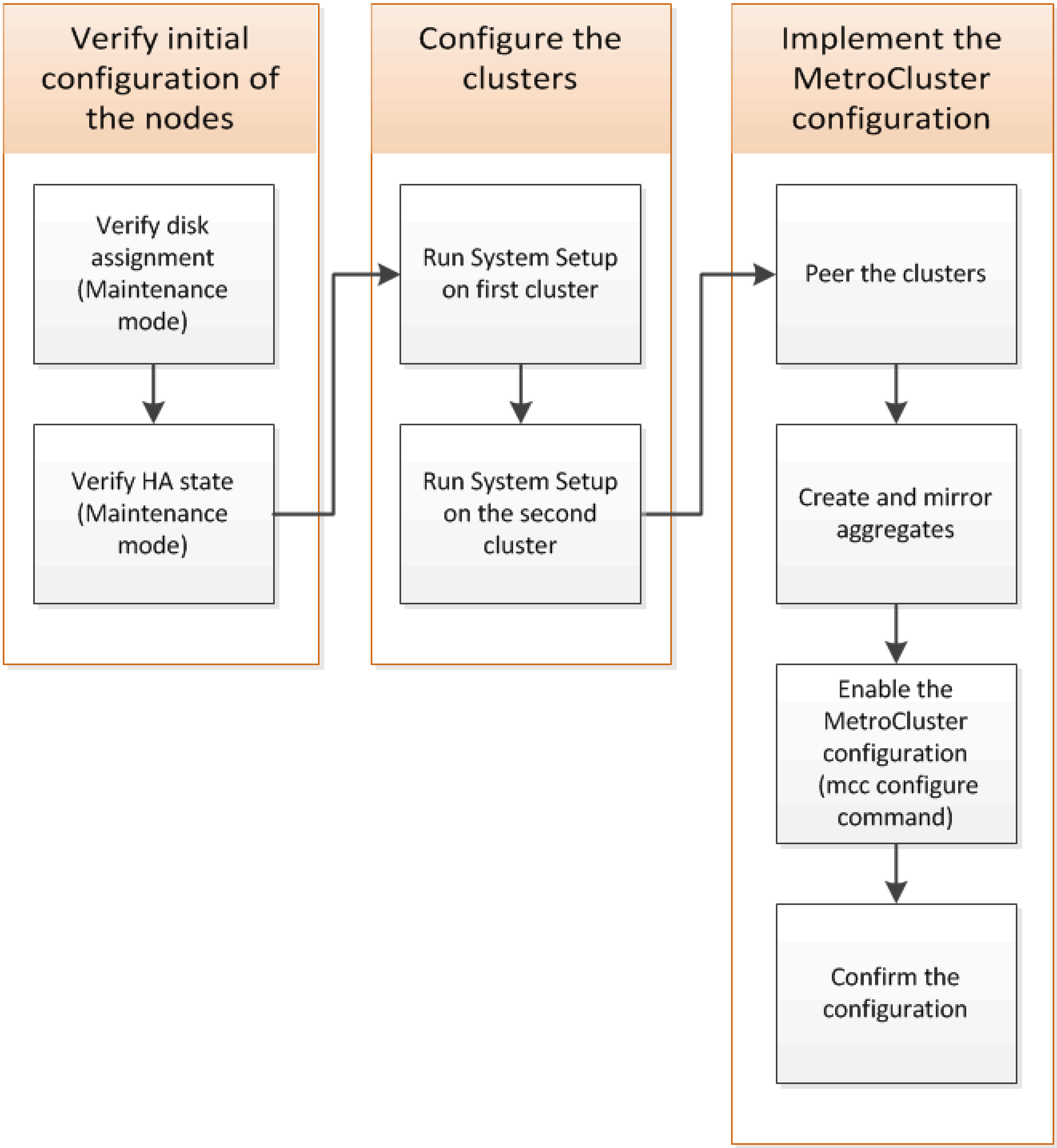
3. Run the fmc_dc utility to ensure that the 7-Mode fabric MetroCluster is functioning correctly.

   You can ignore errors related to Traffic Isolation (TI) zoning and trunking.

4. Repeat the tasks for the second switch fabric.

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. The steps for systems with native disk shelves are slightly different from those for systems with array LUNs.



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 switch information (switched clusters)

When you cable the system, you need a host name and management IP address for each cluster switch. This information is not needed if you are using a two-node switchless cluster or have a two-node MetroCluster configuration (one node at each site).

Cluster switch	Host name	IP address	Network mask	Default gateway
Interconnect 1				
Interconnect 2				
Management 1				
Management 2				

Site A cluster creation information

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

Type of information	Your values
Cluster name Example used in this guide: site_A	
DNS domain	
DNS name servers	
Location	
Administrator password	

Site A node information

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

Node	Port	IP address	Network mask	Default gateway
Node 1 Example used in this guide: controller_A_1				

Node 2Not required if using two-node MetroCluster configuration (one node at each site). Example used in this guide: controller_A_2				

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.

Node	Port	IP address of intercluster LIF	Network mask	Default gateway
Node 1 IC LIF 1				
Node 1 IC LIF 2				
Node 2 IC LIF 1Not required for two-node MetroCluster configurations (one node at each site).				
Node 2 IC LIF 2Not required for two-node MetroCluster configurations (one node at each site).				

Site A time server information

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

Node	Host name	IP address	Network mask	Default gateway
NTP server 1				
NTP server 2				

Site A AutoSupport information

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

Type of information	Your values

From email address		
Mail hosts	IP addresses or names	
Transport protocol	HTTP, HTTPS, or SMTP	
	Proxy server	
Recipient email addresses or distribution lists	Full-length messages	
	Concise messages	
	Partners	

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:

Node	IP address	Network mask	Default gateway
Node 1			
Node 2 Not required for two-node MetroCluster configurations (one node at each site).			

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 switch information (switched clusters)

When you cable the system, you need a host name and management IP address for each cluster switch. This information is not needed if you are using a two-node switchless cluster or you have a two-node MetroCluster configuration (one node at each site).

Cluster switch	Host name	IP address	Network mask	Default gateway
Interconnect 1				
Interconnect 2				
Management 1				

Management 2				

Site B cluster creation information

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

Type of information	Your values
Cluster name Example used in this guide: site_B	
DNS domain	
DNS name servers	
Location	
Administrator password	

Site B node information

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

Node	Port	IP address	Network mask	Default gateway
Node 1 Example used in this guide: controller_B_1				
Node 2 Not required for two-node MetroCluster configurations (one node at each site). Example used in this guide: controller_B_2				

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.

Node	Port	IP address of intercluster LIF	Network mask	Default gateway
Node 1 IC LIF 1				
Node 1 IC LIF 2				
Node 2 IC LIF 1 Not required for two-node MetroCluster configurations (one node at each site).				
Node 2 IC LIF 2 Not required for two-node MetroCluster configurations (one node at each site).				

Site B time server information

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

Node	Host name	IP address	Network mask	Default gateway
NTP server 1				
NTP server 2				

Site B AutoSupport information

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

Type of information		Your values
From email address		
Mail hosts	IP addresses or names	
Transport protocol	HTTP, HTTPS, or SMTP	
	Proxy server	

Recipient email addresses or distribution lists	Full-length messages	
	Concise messages	
	Partners	

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:

Node	IP address	Network mask	Default gateway
Node 1 (controller_B_1)			
Node 2 (controller_B_2) Not required for two-node MetroCluster configurations (one node at each site).			

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.

Configuration step	Standard cluster configuration	MetroCluster configuration
Configure management, cluster, and data LIFs on each node.	Same in both types of clusters	
Configure the root aggregate.	Same in both types of clusters	
Configure nodes in the cluster as HA pairs	Same in both types of clusters	
Set up the cluster on one node in the cluster.	Same in both types of clusters	
Join the other node to the cluster.	Same in both types of clusters	

Create a mirrored root aggregate.	Optional	Required
Peer the clusters.	Optional	Required
Enable the MetroCluster configuration.	Does not apply	Required

Restoring system defaults and configuring the HBA type on a controller module

To ensure a successful MetroCluster installation, reset and restore defaults on the controller modules.

Important

This task is only required for stretch configurations using FC-to-SAS bridges.

Steps

1. At the LOADER prompt, return the environmental variables to their default setting:

   `set-defaults`

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

   a. Boot into Maintenance mode:

      `boot_ontap maint`

   b. Check the current settings of the ports:

      `ucadmin show`

   c. Update the port settings as needed.

If you have this type of HBA and desired mode…	Use this command…
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter_name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter_name`*
FC target	`fcadmin config -t target` *`adapter_name`*
FC initiator	`fcadmin config -t initiator` *`adapter_name`*

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:

   `boot_ontap maint`

5. Verify the changes you made:

If you have this type of HBA…	Use this command…
CNA	`ucadmin show`
FC	`fcadmin show`

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.

> Converting an FC port to an FC-VI port with the ucadmin command is only supported on the FAS8020 and AFF 8020 systems. Converting FC ports to FCVI ports is not supported on any other platform.

Steps

1. Disable the ports:

   `storage disable adapter 1a`

   `storage disable adapter 1b`

```
*> 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`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

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).

```
*> 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`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Shut down the controller, and then reboot into Maintenance mode.
6. Confirm the configuration change:

   `ucadmin show local`

```
Node           Adapter  Mode     Type       Mode     Type       Status
------------   -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
               1a       fc       fcvi       -        -          online
controller_B_1
               1b       fc       fcvi       -        -          online
controller_B_1
               1c       fc       initiator  -        -          online
controller_B_1
               1d       fc       initiator  -        -          online
6 entries were displayed.
```

Verifying disk assignment in Maintenance mode in an eight-node or a four-node configuration

Before fully booting the system to ONTAP, you can optionally boot to Maintenance mode and verify the disk assignment on the nodes. The disks should be assigned to create a fully symmetric active-active configuration, where each pool has an equal number of disks assigned to them.

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.

Disk shelf (sample_shelf_name)…	At site…	Belongs to…	And is assigned to that node's…

Disk shelf 1 (shelf_A_1_1)	Site A	Node A 1	Pool 0
Disk shelf 2 (shelf_A_1_3)			
Disk shelf 3 (shelf_B_1_1)		Node B 1	Pool 1
Disk shelf 4 (shelf_B_1_3)			
Disk shelf 5 (shelf_A_2_1)		Node A 2	Pool 0
Disk shelf 6 (shelf_A_2_3)			
Disk shelf 7 (shelf_B_2_1)		Node B 2	Pool 1
Disk shelf 8 (shelf_B_2_3)			
Disk shelf 1 (shelf_A_3_1)		Node A 3	Pool 0
Disk shelf 2 (shelf_A_3_3)			
Disk shelf 3 (shelf_B_3_1)		Node B 3	Pool 1
Disk shelf 4 (shelf_B_3_3)			
Disk shelf 5 (shelf_A_4_1)		Node A 4	Pool 0
Disk shelf 6 (shelf_A_4_3)			
Disk shelf 7 (shelf_B_4_1)		Node B 4	Pool 1
Disk shelf 8 (shelf_B_4_3)			

Disk shelf 9 (shelf_B_1_2)	Site B	Node B 1	Pool 0
Disk shelf 10 (shelf_B_1_4)			
Disk shelf 11 (shelf_A_1_2)		Node A 1	Pool 1
Disk shelf 12 (shelf_A_1_4)			
Disk shelf 13 (shelf_B_2_2)		Node B 2	Pool 0
Disk shelf 14 (shelf_B_2_4)			
Disk shelf 15 (shelf_A_2_2)		Node A 2	Pool 1
Disk shelf 16 (shelf_A_2_4)			
Disk shelf 1 (shelf_B_3_2)		Node A 3	Pool 0
Disk shelf 2 (shelf_B_3_4)			
Disk shelf 3 (shelf_A_3_2)		Node B 3	Pool 1
Disk shelf 4 (shelf_A_3_4)			
Disk shelf 5 (shelf_B_4_2)		Node A 4	Pool 0
Disk shelf 6 (shelf_B_4_4)			
Disk shelf 7 (shelf_A_4_2)		Node B 4	Pool 1
Disk shelf 8 (shelf_A_4_4)			

Steps

1. Confirm the shelf assignments:

   ```
   disk show -v
   ```

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

Using wildcards in the command enables you to assign all of the disks on a disk shelf with one command. You can identify the disk shelf IDs and bays for each disk with the `storage show disk --x` command.

Assigning disk ownership in non-AFF systems

If the MetroCluster nodes do not have the disks correctly assigned, or if you are using DS460C disk shelves in your configuration, you must assign disks to each of the nodes in the MetroCluster configuration on a shelf-by-shelf basis. You will create a configuration in which each node has the same number of disks in its local and remote disk pools.

About this task

The storage controllers must be in Maintenance mode.

If your configuration does not include DS460C disk shelves, this task is not required if disks were correctly assigned when received from the factory.

> Pool 0 always contains the disks that are found at the same site as the storage system that owns them.

Pool 1 always contains the disks that are remote to the storage system that owns them.

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

Assign these disks in the drawer…	To this node and pool…
0 - 2	Local node’s pool 0
3 - 5	HA partner node’s pool 0
6 - 8	DR partner of the local node’s pool 1
9 - 11	DR partner of the HA partner’s pool 1

This disk assignment pattern ensures that an aggregate is minimally affected in case a drawer goes offline.

Steps

1. If you have not done so, boot each system into Maintenance mode.
2. Assign the disk shelves to the nodes located at the first site (site A):

   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. On the first node, systematically assign the local disk shelves to pool 0 and the remote disk shelves to pool 1:

      ```
      disk assign -shelf local-switch-name:shelf-name.port -p pool
      ```

      If storage controller Controller_A_1 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
```

b. Repeat the process for the second node at the local site, systematically assigning the local disk shelves to pool 0 and the remote disk shelves to pool 1:

`disk assign -shelf local-switch-name:shelf-name.port -p pool`

If storage controller Controller_A_2 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
```

3. Assign the disk shelves to the nodes located at the second site (site B):

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

   `disk assign -shelf local-switch-nameshelf-name -p pool`

   If storage controller Controller_B_1 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

   b. Repeat the process for the second node at the remote site, systematically assigning its local disk shelves to pool 0 and its remote disk shelves to pool 1:

   `disk assign -shelf shelf-name -p pool`

   If storage controller Controller_B_2 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Confirm the shelf assignments:

   `storage show shelf`

5. Exit Maintenance mode:

   `halt`

6. Display the boot menu:

   `boot_ontap menu`

7. On each node, select option **4** to initialize all disks.

Assigning disk ownership in AFF systems

If you are using AFF systems in a configuration with mirrored aggregates and the nodes do not have the disks (SSDs) correctly assigned, you should assign half the disks on each shelf to one local node and the other half of the disks to its HA partner node. You should create a configuration in which each node has the same number of disks in its local and remote disk pools.

About this task

The storage controllers must be in Maintenance mode.

This does not apply to configurations which have unmirrored aggregates, an active/passive configuration, or that have an unequal number of disks in local and remote pools.

This task is not required if disks were correctly assigned when received from the factory.

> ℹ️ Pool 0 always contains the disks that are found at the same site as the storage system that owns them, while Pool 1 always contains the disks that are remote to the storage system that owns them.

Steps

1. If you have not done so, boot each system into Maintenance mode.
2. Assign the disks to the nodes located at the first site (site A):

   You should assign an equal number of disks to each pool.

   a. On the first node, systematically assign half the disks on each shelf to pool 0 and the other half to the HA partner's pool 0:

      `disk assign -disk disk-name -p pool -n number-of-disks`

      If storage controller Controller_A_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

b. Repeat the process for the second node at the local site, systematically assigning half the disks on each shelf to pool 1 and the other half to the HA partner's pool 1:

`disk assign -disk disk-name -p pool`

If storage controller Controller_A_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Assign the disks to the nodes located at the second site (site B):

   You should assign an equal number of disks to each pool.

   a. On the first node at the remote site, systematically assign half the disks on each shelf to pool 0 and the other half to the HA partner's pool 0:

   `disk assign -disk disk-name -p pool`

   If storage controller Controller_B_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

   b. Repeat the process for the second node at the remote site, systematically assigning half the disks on each shelf to pool 1 and the other half to the HA partner's pool 1:

   `disk assign -disk disk-name -p pool`

   If storage controller Controller_B_2 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Confirm the disk assignments:

   `storage show disk`

5. Exit Maintenance mode:
   `halt`

6. Display the boot menu:

   `boot_ontap menu`

7. On each node, select option **4** to initialize all disks.

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.

Disk shelf (example name)…	At site…	Belongs to…	And is assigned to that node's…
Disk shelf 1 (shelf_A_1_1)	Site A	Node A 1	Pool 0
Disk shelf 2 (shelf_A_1_3)	Disk shelf 3 (shelf_B_1_1)	Node B 1	Pool 1
Disk shelf 4 (shelf_B_1_3)	Disk shelf 9 (shelf_B_1_2)	Site B	Node B 1
Pool 0	Disk shelf 10 (shelf_B_1_4)	Disk shelf 11 (shelf_A_1_2)	Node A 1

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

Assign these disks in the drawer…	To this node and pool…
1 - 6	Local node's pool 0
7 - 12	DR partner's pool 1

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:

   `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:

      `disk assign -shelf disk_shelf_name -p pool`

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

      ```
      *> 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:

      `disk assign -shelf disk_shelf_name -p pool`

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

      ```
      *> 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:

```
disk show -v
```

Verifying and configuring the HA state of components in Maintenance mode

When configuring a storage system in a MetroCluster configuration, you must make sure that the high-availability (HA) state of the controller module and chassis components is mcc or mcc-2n so that these components boot properly.

Before you begin

The system must be in Maintenance mode.

About this task

This task is not required on systems that are received from the factory.

Steps

1. In Maintenance mode, display the HA state of the controller module and chassis:

   ```
   ha-config show
   ```

   The correct HA state depends on your MetroCluster configuration.

Number of controllers in the MetroCluster configuration	HA state for all components should be…
Eight- or four-node MetroCluster FC configuration	mcc
Two-node MetroCluster FC configuration	mcc-2n
MetroCluster IP configuration	mccip

2. If the displayed system state of the controller is not correct, set the HA state for the controller module:

Number of controllers in the MetroCluster configuration	Command
Eight- or four-node MetroCluster FC configuration	ha-config modify controller mcc
Two-node MetroCluster FC configuration	ha-config modify controller mcc-2n
MetroCluster IP configuration	ha-config modify controller mccip

3. If the displayed system state of the chassis is not correct, set the HA state for the chassis:

Number of controllers in the MetroCluster configuration	Command
Eight- or four-node MetroCluster FC configuration	ha-config modify chassis mcc

Two-node MetroCluster FC configuration	ha-config modify chassis mcc-2n
MetroCluster IP configuration	ha-config modify chassis mccip

Steps

1. Boot the node to ONTAP:

   ```
   boot_ontap
   ```

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

Setting up ONTAP

You must set up ONTAP on each controller module.

If you need to netboot the new controllers, see Netbooting the new controller modules in the *MetroCluster Upgrade, Transition, and Expansion Guide*.

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 Cluster Setup wizard, and use the cluster setup command 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.

   > You must repeat this step on the node at the disaster recovery (DR) site.

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

```
::> 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.

This system will send event messages and periodic 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}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address [10.101.01.01]:

Enter the node management interface netmask [101.010.101.0]:
Enter the node management interface default gateway [10.101.01.0]:



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

2. Create a new cluster:

   `create`

3. Choose whether the node is to be used as a single node cluster.

```
Do you intend for this node to be used as a single node cluster? {yes,
no} [yes]:
```

4. Accept the system default `yes` by pressing Enter, or enter your own values by typing `no`, and then pressing

Enter.

5. 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.

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

   `cluster show`

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

```
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.

Software setup

Setting up ONTAP in an eight-node or four-node MetroCluster configuration

After you boot each node, you are prompted to run the System Setup tool to perform basic node and cluster configuration. After configuring the cluster, you return to the ONTAP CLI to create aggregates and create the MetroCluster configuration.

Before you begin

You must have cabled the MetroCluster configuration.

About this task

This task is for eight-node or four-node MetroCluster configurations using native NetApp storage.

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

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

This procedure uses the System Setup tool. If desired, you can use the CLI cluster setup wizard instead.

Steps

1. If you have not already done so, power up each node and let them boot completely.

   If the system is in Maintenance mode, issue the halt command to exit Maintenance mode, and then issue the following command from the LOADER prompt:

   `boot_ontap`

The output should be similar to the following:

```
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.
.
.
.
```

2. Enable the AutoSupport tool by following the directions provided by the system.
3. Respond to the prompts to configure the node management interface.

   The prompts are similar to the following:

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Confirm that nodes are configured in high-availability mode:

   `storage failover show -fields mode`

   If not, you must issue the following command on each node and reboot the node:

   `storage failover modify -mode ha -node localhost`

   This command configures high availability mode but does not enable storage failover. Storage failover is automatically enabled when the MetroCluster configuration is performed later in the configuration process.

5. Confirm that you have four ports configured as cluster interconnects:

   `network port show`

   The following example shows output for cluster_A:

```
cluster_A::> network port show
                                                                    Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU     Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **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
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **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
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. If you are creating a two-node switchless cluster (a cluster without cluster interconnect switches), enable the switchless-cluster networking mode:
   a. Change to the advanced privilege level:

      `set -privilege advanced`

      You can respond `y` when prompted to continue into advanced mode. The advanced mode prompt appears (*>).

   b. Enable switchless-cluster mode: `network options switchless-cluster modify -enabled true`
   c. Return to the admin privilege level: `set -privilege admin`
7. Launch the System Setup tool as directed by the information that appears on the system console after the initial boot.
8. Use the System Setup tool to configure each node and create the cluster, but do not create aggregates.

   > You create mirrored aggregates in later tasks.

Return to the ONTAP command-line interface and complete the MetroCluster configuration by performing the tasks that follow.

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.

Related information

Cluster and SVM peering express configuration

Considerations when using dedicated ports

Considerations when sharing data ports

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.

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.

   The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                                Speed
(Mbps)
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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

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.

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

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

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
```

The following example assigns ports e0e and e0f to the failover group intercluster01 on the system SVMcluster01:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verify that the failover group was created:

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

For complete command syntax, see the man page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

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

ONTAP version	**Command**
9.6 and later	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home-port port -address port_IP -netmask netmask -failover -group failover_group`

9.5 and earlier	`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.

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

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-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 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs "`cluster01_icl01`" and "`cluster01_icl02`" on the SVMe0e port will fail over to the e0f port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Related information

Considerations when using dedicated ports

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.

   The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                                    Speed
(Mbps)
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:

In ONTAP 9.6 and later:
`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home-port port -address port_IP -netmask netmask`
In ONTAP 9.5 and earlier:
`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.

The following example creates intercluster LIFs cluster01_icl01 and cluster01_icl02:

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

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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:

In ONTAP 9.6 and later:

```
network interface show -service-policy default-intercluster -failover
```

In ONTAP 9.5 and earlier:

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

For complete command syntax, see the man page.

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

```
cluster01::> network interface show -service-policy default-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 information

Considerations when sharing data ports

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.

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.

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

```
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.

   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:

   ```
   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`

```
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`

```
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
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             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.

   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:

   ```
   cluster02::> cluster peer create -peer-addrs 192.168.2.201,192.168.2.202
   Enter the passphrase:
   Please enter the passphrase again:
   ```

   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.

   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
   Please confirm the passphrase:
   Please confirm the passphrase again:
   ```

   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.

```
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.

```
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
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             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
```

> 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`

   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

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.
- 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. See 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

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.

    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

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.

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:

   `storage disk show -spare -owner node_name`

2. Create the aggregate:

   `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.

     The following command creates a unmirrored aggregate with 10 disks:

   ```
   controller_A_1::> storage aggregate create aggr1_controller_A_1
   -diskcount 10 -node controller_A_1
   [Job 15] Job is queued: Create aggr1_controller_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`

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.

About this task

Additional data aggregates can be either mirrored or unmirrored.

You can verify this with the storage aggregate show command.

> If you want to use a single mirrored data aggregate, then see Step 1 in "Configure the MetroCluster software in ONTAP" for instructions.

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

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.

The `metrocluster configure` command automatically pairs the two nodes with the lowest system IDs in each of the two clusters as disaster recovery (DR) partners. In a four-node MetroCluster configuration, there are two DR partner pairs. The second DR pair is created from the two nodes with higher system IDs.

Steps

1. Configure the MetroCluster in the following format:

If your MetroCluster configuration has…	Then do this…
Multiple data aggregates	From any node's prompt, configure MetroCluster: `metrocluster configure node-name`

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`

> 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:

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

[Job 121] Job succeeded: Configure is successful.
```

2. Verify the networking status on site A:

   `network port show`

   The following example shows the network port usage on a four-node MetroCluster configuration:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

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

   a. Verify the configuration from site A:

      `metrocluster show`

```
cluster_A::> metrocluster show

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Verify the configuration from site B:

      `metrocluster show`

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

Configuring in-order delivery or out-of-order delivery of frames on ONTAP software

You must configure either in-order delivery (IOD) or out-of-order delivery (OOD) of frames according to the fibre channel (FC) switch configuration. If the FC switch is configured for IOD, then the ONTAP software must be configured for IOD. Similarly, if the FC switch is configured for OOD, then ONTAP must be configured for OOD.

Steps

1. Configure ONTAP to operate either IOD or OOD of frames.
   - By default, IOD of frames is enabled in ONTAP. To check the configuration details:
     a. Enter advanced mode:

        `set advanced`

     b. Verify the settings:

        `metrocluster interconnect adapter show`

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                             Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address
Port Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI    Up    false    18.0.0.2
6b
mcc4-b1      mlx4_0          IB       Down  false    192.0.5.193
ib2a
mcc4-b1      mlx4_0          IB       Up    false    192.0.5.194
ib2b
mcc4-b2      fcvi_device_0   FC-VI    Up    false    17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI    Up    false    18.0.1.2
6b
mcc4-b2      mlx4_0          IB       Down  false    192.0.2.9
ib2a
mcc4-b2      mlx4_0          IB       Up    false    192.0.2.10
ib2b
8 entries were displayed.
```

- The following steps must be performed on each node to configure OOD of frames:
  a. Enter advanced mode:

     `set advanced`

  b. Verify the MetroCluster configuration settings:

     `metrocluster interconnect adapter show`

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                             Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address
Port Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI    Up    false    17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI    Up    false    18.0.0.2
6b
mcc4-b1      mlx4_0          IB       Down  false    192.0.5.193
ib2a
mcc4-b1      mlx4_0          IB       Up    false    192.0.5.194
ib2b
mcc4-b2      fcvi_device_0   FC-VI    Up    false    17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI    Up    false    18.0.1.2
6b
mcc4-b2      mlx4_0          IB       Down  false    192.0.2.9
ib2a
mcc4-b2      mlx4_0          IB       Up    false    192.0.2.10
ib2b
8 entries were displayed.
```

c. Enable OOD on node “mcc4-b1” and node “mcc4-b2”:

`metrocluster interconnect adapter modify -node node name -is-ood-enabled true`

```
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b1 -is-ood-enabled true
mcc4-b12_siteB::*> metrocluster interconnect adapter modify -node
mcc4-b2 -is-ood-enabled true
```

d. Verify the settings:

`metrocluster interconnect adapter show`

```
mcc4-b12_siteB::*> metrocluster interconnect adapter show
                             Adapter Link   Is OOD
Node         Adapter Name    Type    Status Enabled? IP Address
Port Number
------------ --------------- ------- ------ -------- -----------
-----------
mcc4-b1      fcvi_device_0   FC-VI   Up     true      17.0.1.2
6a
mcc4-b1      fcvi_device_1   FC-VI   Up     true      18.0.0.2
6b
mcc4-b1      mlx4_0          IB      Down   false     192.0.5.193
ib2a
mcc4-b1      mlx4_0          IB      Up     false     192.0.5.194
ib2b
mcc4-b2      fcvi_device_0   FC-VI   Up     true      17.0.2.2
6a
mcc4-b2      fcvi_device_1   FC-VI   Up     true      18.0.1.2
6b
mcc4-b2      mlx4_0          IB      Down   false     192.0.2.9
ib2a
mcc4-b2      mlx4_0          IB      Up     false     192.0.2.10
ib2b
8 entries were displayed.
```

Configuring SNMPv3 in a MetroCluster configuration

The authentication and privacy protocols on the switches and on the ONTAP system must be the same.

About this task

ONTAP currently supports AES-128 and AES-256 encryption.

Steps

1. Create an SNMP user for each switch from the controller prompt:

   `security login create`

   ```
   Controller_A_1::> security login create -user-or-group-name snmpv3user
   -application snmp -authentication-method usm -role none -remote-switch
   -ipaddress 10.10.10.10
   ```

2. Respond to the following prompts as required at your site:

```
Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256) [none]: sha

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128) [none]:
aes128

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:
```

> The same username can be added to different switches with different IP addresses.

3. Create an SNMP user for the rest of the switches.

   The following example shows how to create a username for a switch with the IP address 10.10.10.11.

   ```
   Controller_A_1::> security login create -user-or-group-name snmpv3user
   -application snmp -authentication-method usm -role none -remote-switch
   -ipaddress 10.
   10.10.11
   ```

4. Check that there is one login entry for each switch:

   `security login show`

```
Controller_A_1::> security login show -user-or-group-name snmpv3user
-fields remote-switch-ipaddress

vserver      user-or-group-name application authentication-method
remote-switch-ipaddress

------------ ------------------ ----------- ---------------------
-----------------------

node_A_1 SVM 1 snmpv3user     snmp        usm
10.10.10.10

node_A_1 SVM 2 snmpv3user     snmp        usm
10.10.10.11

node_A_1 SVM 3 snmpv3user    snmp        usm
10.10.10.12

node_A_1 SVM 4 snmpv3user     snmp        usm
10.10.10.13

4 entries were displayed.
```

5. Configure SNMPv3 on the switches from the switch prompt:

   `snmpconfig --set snmpv3`

   If you require RO access, after "User (ro):" specify the "snmpv3user" as shown in the example:

```
Switch-A1:admin> snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] true
SNMPv3 user configuration(snmp user not configured in FOS user database
will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00:00]
User (ro): [snmpuser2] snmpv3user
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [2]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [3]
```

   The example shows how to configure a read-only user. You can adjust the RW users if needed. You should also set passwords on unused accounts to secure them and use the best encryption available in your ONTAP release.

6. Configure encryption and passwords on the remaining switch users as required on your site.

Configuring MetroCluster components for health monitoring

You must perform some special configuration steps before monitoring the components in a MetroCluster configuration.

About this task

These tasks apply only to systems with FC-to-SAS bridges.

> - You should place bridges and a node management LIF in a dedicated network to avoid interference from other sources.
> - If you use a dedicated network for Health Monitoring, then each node must have a node management LIF in that dedicated network.

Configuring the MetroCluster FC switches for health monitoring

In a fabric-attached MetroCluster configuration, you must perform some additional configuration steps to monitor the FC switches.

> Starting with ONTAP 9.8, the `storage switch` command is replaced with `system switch`. The following steps show the `storage switch` command, but if you are running ONTAP 9.8 or later, the `system switch` command is preferred.

Steps

1. Add a switch with an IP address to each MetroCluster node:

   `storage switch add -address ipaddress`

   This command must be repeated on all four switches in the MetroCluster configuration.

   > Brocade 7840 FC switches and all alerts are supported in health monitoring, except NoISLPresent_Alert

   The following example shows the command to add a switch with IP address 10.10.10.10:

   ```
   controller_A_1::> storage switch add -address 10.10.10.10
   ```

2. Verify that all switches are properly configured:

   `storage switch show`

   It might take up to 15 minutes to reflect all data due to the 15-minute polling interval.

   The following example shows the command given to verify that the MetroCluster FC switches are configured:

```
controller_A_1::> storage switch show
Fabric           Switch Name     Vendor  Model        Switch WWN
Status
---------------- --------------- ------- ------------ ----------------
------
1000000533a9e7a6 brcd6505-fcs40  Brocade Brocade6505  1000000533a9e7a6
OK
1000000533a9e7a6 brcd6505-fcs42  Brocade Brocade6505  1000000533d3660a
OK
1000000533ed94d1 brcd6510-fcs44  Brocade Brocade6510  1000000533eda031
OK
1000000533ed94d1 brcd6510-fcs45  Brocade Brocade6510  1000000533ed94d1
OK
4 entries were displayed.

controller_A_1::>
```

If the worldwide name (WWN) of the switch is shown, the ONTAP health monitor can contact and monitor the FC switch.

Related information

System administration

Configuring FC-to-SAS bridges for health monitoring

In systems running ONTAP versions prior to 9.8, 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.
- Starting with ONTAP 9.8, FC-to-SAS bridges are monitored via in-band connections by default, and additional configuration is not required.

> Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

Steps

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

ONTAP version	Command
9.5 and later	`storage bridge add -address 0.0.0.0 -managed-by in-band -name bridge-name`

9.4 and earlier	`storage bridge add -address bridge-ip-address -name bridge-name`

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.

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

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status
Vendor Model                Bridge WWN
------------------  ------------- ------------  --------------
------ -----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

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.

1. Check the configuration:

   `metrocluster check run`

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.

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

Node                    Aggregate                   Check
```

```
Result
---------------      --------------------      ---------------------
---------
controller_A_1       controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                     controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                     controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok


controller_A_2       controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                     controller_A_2_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                     controller_A_2_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
```

```
ok

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

Cluster                     Check                              Result
--------------------- ------------------------------- ---------
mccint-fas9000-0102
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
mccint-fas9000-0304
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
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.

> ⓘ 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 local HA operation

If you have a four-node MetroCluster configuration, you should verify the operation of the local HA pairs in the MetroCluster configuration. This is not required for two-node configurations.

About this task

Two-node MetroCluster configurations do not consist of local HA pairs and this task does not apply.

The examples in this task use standard naming conventions:

- cluster_A
  - controller_A_1
  - controller_A_2
- cluster_B
  - controller_B_1
  - controller_B_2

Steps

1. On cluster_A, perform a failover and giveback in both directions.
   a. Confirm that storage failover is enabled:

      `storage failover show`

      The output should indicate that takeover is possible for both nodes:

      ```
      cluster_A::> storage failover show
                                    Takeover
      Node           Partner        Possible State Description
      -------------- -------------- -------- ---------------------------
      controller_A_1 controller_A_2 true     Connected to controller_A_2

      controller_A_2 controller_A_1 true     Connected to controller_A_1
      2 entries were displayed.
      ```

   b. Take over controller_A_2 from controller_A_1:

      `storage failover takeover controller_A_2`

      You can use the `storage failover show-takeover` command to monitor the progress of the takeover operation.

   c. Confirm that the takeover is complete:

```
storage failover show
```

The output should indicate that controller_A_1 is in takeover state, meaning that it has taken over its HA partner:

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- -----------------
controller_A_1 controller_A_2 false    In takeover

controller_A_2 controller_A_1 -        Unknown
2 entries were displayed.
```

d. Give back controller_A_2:

```
storage failover giveback controller_A_2
```

You can use the `storage failover show-giveback` command to monitor the progress of the giveback operation.

e. Confirm that storage failover has returned to a normal state:

```
storage failover show
```

The output should indicate that takeover is possible for both nodes:

```
cluster_A::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- -------- ---------------------------
controller_A_1 controller_A_2 true     Connected to controller_A_2

controller_A_2 controller_A_1 true     Connected to controller_A_1
2 entries were displayed.
```

f. Repeat the previous substeps, this time taking over controller_A_1 from controller_A_2.

2. Repeat the preceding steps on cluster_B.

Related information

High-availability configuration

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

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*.

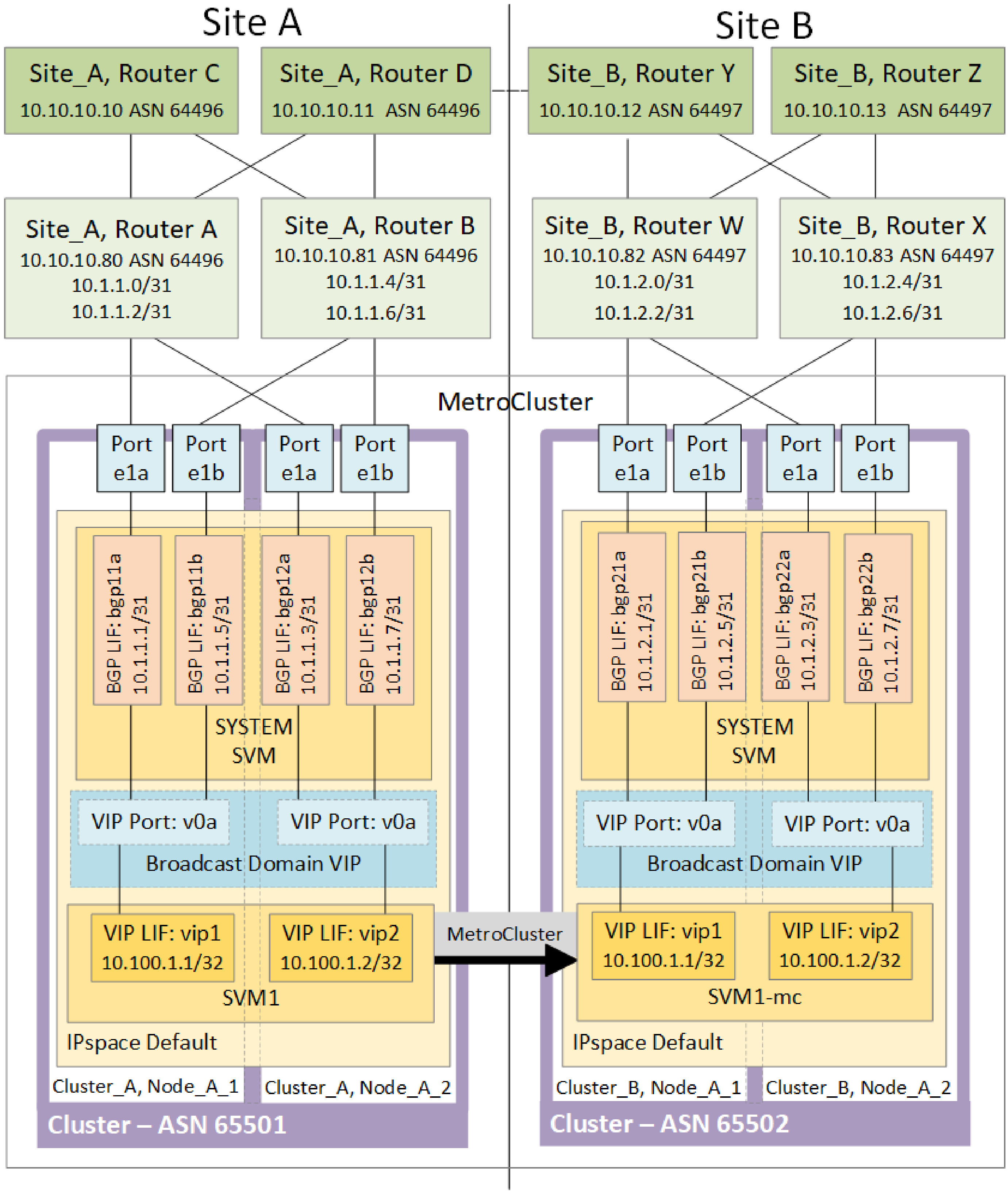
Related information

System administration

Considerations for using virtual IP and Border Gateway Protocol with a MetroCluster configuration

Starting with ONTAP 9.5, ONTAP supports layer 3 connectivity using virtual IP (VIP) and Border Gateway Protocol (BGP). The combination VIP and BGP for redundancy in the front-end networking with the back-end MetroCluster redundancy provides a layer 3 disaster recovery solution.

Review the following guidelines and illustration when planning your layer 3 solution. For details on implementing VIP and BGP in ONTAP, refer to Configure virtual IP LIFs.



ONTAP limitations

ONTAP does not automatically verify that all nodes on both sites of the MetroCluster configuration are configured with BGP peering.

ONTAP does not perform route aggregation but announces all individual virtual LIF IPs as unique host routes at all times.

ONTAP does not support true AnyCast — only a single node in the cluster presents a specific virtual LIF IP (but is accepted by all physical interfaces, regardless of whether they are BGP LIFs, provided the physical port is part of the correct IPspace). Different LIFs can migrate independently of each other to different hosting nodes.

Guidelines for using this Layer 3 solution with a MetroCluster configuration

You must configure your BGP and VIP correctly to provide the required redundancy.

Simpler deployment scenarios are preferred over more complex architectures (for example, a BGP peering router is reachable across an intermediate, non-BGP router). However, ONTAP does not enforce network design or topology restrictions.

VIP LIFs only cover the frontend/data network.

Depending on your version of ONTAP, you must configure BGP peering LIFs in the node SVM, not the system or data SVM. In 9.8, the BGP LIFs are visible in the cluster (system) SVM and the node SVMs are no longer present.

Each data SVM requires the configuration of all potential first hop gateway addresses (typically, the BGP router peering IP address), so that the return data path is available if a LIF migration or MetroCluster failover occurs.

BGP LIFs are node specific, similar to intercluster LIFs — each node has a unique configuration, which does not need to be replicated to DR site nodes.

configured, the existence of the v0a (v0b and so on.) continuously validates the connectivity, guaranteeing that a LIF migrate or failover succeeds (unlike L2, where a broken configuration is only visible after the outage).

A major architectural difference is that clients should no longer share the same IP subnet as the VIP of data SVMs. An L3 router with appropriate enterprise grade resiliency and redundancy features enabled (for example, VRRP/HSRP) should be on the path between storage and clients for the VIP to operate correctly.

The reliable update process of BGP allows for smoother LIF migrations because they are marginally faster and have a lower chance of interruption to some clients

You can configure BGP to detect some classes of network or switch misbehaviors faster than LACP, if configured accordingly.

External BGP (EBGP) uses different AS numbers between ONTAP node(s) and peering routers and is the preferred deployment to ease route aggregation and redistribution on the routers. Internal BGP (IBGP) and the use of route reflectors is not impossible but outside the scope of a straightforward VIP setup.

After deployment, you must check that the data SVM is accessible when the associated virtual LIF is migrated between all nodes on each site (including MetroCluster switchover) to verify the correct configuration of the static routes to the same data SVM.

VIP works for most IP-based protocols (NFS, SMB, iSCSI).

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 the command is issued from will switch over the partner site.

For MetroCluster IP configurations:

- For ONTAP 9.4 and earlier:
  - Mirrored aggregates will become degraded after the negotiated switchover.
- For ONTAP 9.5 and later:
  - Mirrored aggregates will remain in normal state if the remote storage is accessible.
  - Mirrored aggregates will become degraded after the negotiated switchover if access to the remote storage is lost.
- For ONTAP 9.8 and later:
  - Unmirrored aggregates that are located at the disaster site will become unavailable if access to the remote storage is lost. This might lead to a controller outage.

Steps

1. Confirm that all nodes are in the configured state and normal mode:

   `metrocluster node show`

   ```
   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`

```
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`

```
cluster_A::>  metrocluster node show

Cluster                        Configuration State    Mode
------------------------------ ----------------------
------------------------
Local: cluster_A                configured             switchover
Remote: cluster_B               not-reachable          -
              configured             normal
```

4. Confirm that the switchover operation was successful:

   `metrocluster operation show`

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

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.

Steps

1. Verify that healing is completed:

   `metrocluster node show`

   The following example shows the successful completion of the command:

```
cluster_A::> metrocluster node show
DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1          configured     enabled   heal roots
completed
      cluster_B
              node_B_2          unreachable    -         switched over
42 entries were displayed.metrocluster operation show
```

2. Verify that all aggregates are mirrored:

   `storage aggregate show`

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

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                              mirrored,
                                                              normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                              mirrored,
                                                              normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                              mirrored,
                                                              normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

3. Boot the nodes from the disaster site.
4. Check the status of switchback recovery:

`metrocluster node show`

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
             node_A_1            configured     enabled   heal roots
completed
      cluster_B
             node_B_2            configured     enabled   waiting for
switchback
                                                          recovery
2 entries were displayed.
```

5. Perform the switchback:

   `metrocluster switchback`

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

6. Confirm the status of the nodes:

   `metrocluster node show`

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

   2 entries were displayed.
   ```

7. Confirm the status of the `metrocluster operation`:

   `metrocluster operation show`

   The output should show a successful state.

   ```
   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.

> Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

Steps

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

   `storage bridge show`

```
cluster_A::> storage bridge show

                                                            Is
Monitor
Bridge     Symbolic Name Vendor  Model     Bridge WWN       Monitored
Status
---------- ------------- ------- --------- ---------------- ---------
-------
ATTO_10.65.57.145
         bridge_A_1    Atto    FibreBridge 6500N
                                           200000108662d46c true
error
```

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

   `storage disk error show`

```
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 PDUs are disconnected.
- No failover or loss of service should occur.

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 following commands:

   `system environment sensors show -state fault`

   `storage shelf show -errors`

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

Node Sensor              State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- --------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
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 a switch fabric failure

You can disable a switch fabric to show that data availability is not affected by the loss.

About this task

This test should take about 15 minutes.

The expected result of this procedure is that disabling a fabric results in all cluster interconnect and disk traffic flowing to the other fabric.

In the examples shown, switch fabric 1 is disabled. This fabric consists of two switches, one at each MetroCluster site:

- FC_switch_A_1 on cluster_A

- FC_switch_B_1 on cluster_B

Steps

1. Disable connectivity to one of the two switch fabrics in the MetroCluster configuration:
   a. Disable the first switch in the fabric:

      `switchdisable`

      ```
      FC_switch_A_1::> switchdisable
      ```

   b. Disable the second switch in the fabric:

      `switchdisable`

      ```
      FC_switch_B_1::> switchdisable
      ```

2. Monitor the result on the console of the controller modules.

   You can use the following commands to check the cluster nodes to make sure that all data is still being served. The command output shows missing paths to disks. This is expected.

   - vserver show
   - network interface show
   - aggr show
   - system node runnodename-command storage show disk -p
   - storage disk error show

3. Reenable connectivity to one of the two switch fabrics in the MetroCluster configuration:
   a. Reenable the first switch in the fabric:

      `switchenable`

      ```
      FC_switch_A_1::> switchenable
      ```

   b. Reenable the second switch in the fabric:

      `switchenable`

      ```
      FC_switch_B_1::> switchenable
      ```

4. Wait at least 10 minutes and then repeat the above steps on the other switch fabric.

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`

```
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`

```
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*

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

cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

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
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

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.

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

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 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)
                                                              Usable
Physical
     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)
                                                              Usable
Physical
     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)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                              Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   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`

   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,

mirror

degraded
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,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(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)
                                                              Usable
Physical
     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 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                              Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                      -    -          -  827.7GB
- (failed)
     parity   FAILED                      -    -          -  827.7GB
- (failed)
     data     FAILED                      -    -          -  827.7GB
- (failed)
     data     FAILED                      -    -          -  827.7GB
- (failed)
     data     FAILED                      -    -          -  827.7GB
- (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                              Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                     0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     data     2.30.21                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                       0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

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*
```

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

cluster_A::> vserver show -type data
                              Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

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
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Physically power on the shelf.

   Resynchronization starts automatically.

9. Verify that resynchronization has started:

   `storage aggregate show`

   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`

    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_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,

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
```

Considerations when removing MetroCluster configurations

You can remove the MetroCluster configuration from all nodes in the MetroCluster configuration or 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.

You cannot reverse the MetroCluster unconfiguration. This process should only be done with the assistance of technical support.

Planning and installing a MetroCluster configuration with array LUNs

If you are using array LUNs in your MetroCluster configuration, you must plan the installation and follow the specific procedures for such a configuration. You can set up a MetroCluster configuration with either a mix of array LUNs and native disk shelves or only array LUNs.

Planning for a MetroCluster configuration with array LUNs

Creating a detailed plan for your MetroCluster configuration helps you understand the unique requirements for a MetroCluster configuration that uses LUNs on storage arrays. Installing a MetroCluster configuration involves connecting and configuring a number of devices, which might be done by different people. Therefore, the plan also helps you communicate with other people involved in the installation.

Supported MetroCluster configuration with array LUNs

You can set up either a MetroCluster configuration with array LUNs. Both stretch and fabric-attached configurations are supported. AFF systems are not supported with array LUNs.

The features supported on the MetroCluster configurations vary with the configuration types. The following table lists the features supported on the different types of MetroCluster configurations with array LUNs:

Feature	Fabric-attached configurations			Stretch configurations
	Eight-node	**Four-node**	**Two-node**	**Two-node**
Number of controllers	Eight	Four	Two	Two
Uses an FC switch storage fabric	Yes	Yes	Yes	Yes
Uses FC-to-SAS bridges	Yes	Yes	Yes	Yes
Supports local HA	Yes	Yes	No	No
Supports automatic switchover	Yes	Yes	Yes	Yes

Related information

Differences between the ONTAP MetroCluster configurations

Requirements for a MetroCluster configuration with array LUNs

The ONTAP systems, storage arrays, and FC switches used in MetroCluster configurations must meet the requirements for such types of configurations. In addition, you must also consider the SyncMirror requirements for MetroCluster configurations with array LUNs.

Requirements for ONTAP systems

- The ONTAP systems must be identified as supported for MetroCluster configurations.

  In the NetApp Interoperability Matrix Tool (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.

  > You must refer to the alert details associated with any configuration that you select in the Interoperability Matrix.

- All the ONTAP systems in a MetroCluster configuration must be of the same model.
- FC-VI adapters must be installed in the appropriate slots for each ONTAP system, depending on the model.

  NetApp Hardware Universe

Requirements for storage arrays

- The storage arrays must be identified as supported for MetroCluster configurations.

  NetApp Interoperability Matrix Tool

- The storage arrays in the MetroCluster configuration must be symmetric:
  - The two storage arrays must be from the same supported vendor family and have the same firmware version installed.

    FlexArray virtualization implementation for NetApp E-Series storage

    FlexArray virtualization implementation for third-party storage

  - Disk types (for example, SATA, SSD, or SAS) used for mirrored storage must be the same on both storage arrays.
  - The parameters for configuring storage arrays, such as RAID type and tiering, must be the same across both sites.

Requirements for FC switches

- The switches and switch firmware must be identified as supported for MetroCluster configurations.

  NetApp Interoperability Matrix Tool

- Each fabric must have two FC switches.

- Each ONTAP system must be connected to storage using redundant components so that there is redundancy in case of device and path failures.
- FAS9000 storage systems support up to eight ISLs per fabric. Other storage system models support up to four ISLs per fabric.

The switches must use the MetroCluster basic switch configuration, ISL settings, and FC-VI configurations.

Configuring the Cisco or Brocade FC switches manually

SyncMirror requirements

- SyncMirror is required for a MetroCluster configuration.
- Two separate storage arrays, one at each site, are required for the mirrored storage.
- Two sets of array LUNs are required.

  One set is required for the aggregate on the local storage array (pool0) and another set is required at the remote storage array for the mirror of the aggregate (the other plex of the aggregate, pool1).

  The array LUNs must be of the same size for mirroring the aggregate.
- Unmirrored aggregates are also supported in the MetroCluster configuration.

  They are not protected in the event of a site disaster.

Installing and cabling the MetroCluster components in a configuration with array LUNs

For setting up a MetroCluster configuration with array LUNs, you must cable the storage controllers to the FC switches and cable the ISLs to link the sites. In addition, you must cable the storage arrays to the FC switches.

Racking the hardware components in a MetroCluster configuration with array LUNs

You must ensure that the hardware components required to set up a MetroCluster configuration with array LUNs are properly racked.

About this task

You must perform this task at both the MetroCluster sites.

Steps

1. Plan 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 systems are not supported with array LUNs.

AFF A700 and FAS9000 Installation and setup

FAS8200 Systems Installation and Setup Instructions

Installation and Setup Instructions FAS8040/FAS8060 Systems

Installation and setup Instructions FAS80xx Systems with I/O Expansion Modules

Installation and Setup Instructions FAS8020 systems

Installation and Setup Instructions 62xx Systems

Installation and Setup Instructions 32xx Systems

4. Install the FC switches in the rack or cabinet.

Preparing a storage array for use with ONTAP systems

Before you can begin setting up ONTAP systems in a MetroCluster configuration with array LUNs, the storage array administrator must prepare the storage for use with ONTAP.

Before you begin

The storage arrays, firmware, and switches that you plan to use in the configuration must be supported by the specific ONTAP version.

- NetApp Interoperability (IMT)

  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.

- NetApp Hardware Universe

About this task

You must coordinate with the storage array administrator to perform this task on the storage array.

Steps

1. Create LUNs on the storage array depending on the number of nodes in the MetroCluster configuration.

   Each node in the MetroCluster configuration requires array LUNs for the root aggregate, data aggregate, and spares.

2. Configure parameters on the storage array that are required to work with ONTAP.
   - FlexArray virtualization implementation for third-party storage
   - FlexArray virtualization implementation for NetApp E-Series storage

Switch ports required for a MetroCluster configuration with array LUNs

When you are connecting ONTAP systems to FC switches for setting up a MetroCluster configuration with array LUNs, you must connect FC-VI and HBA ports from each controller to specific switch ports.

If you are using both array LUNs and disks in the MetroCluster configuration, you must ensure that the controller ports are connected to the switch ports recommended for configuration with disks, and then use the remaining ports for configuration with array LUNs.

The following table lists the specific FC switch ports to which you must connect the different controller ports in an eight-node MetroCluster configuration with array LUNs.

Overall cabling guidelines with array LUNs

You should be aware of the following guidelines when using the cabling tables:

- The Brocade and Cisco switches use different port numbering:
  - On Brocade switches, the first port is numbered 0.
  - On Cisco switches, the first port is numbered 1.
- The cabling is the same for each FC switch in the switch fabric.
- FAS8200 storage systems 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.
- FAS9000 storage systems require four FC-VI ports. The following tables show cabling for the FC switches with four FC-VI ports on each controller.

  For other storage systems, use the cabling shown in the tables but ignore the cabling for FC-VI ports c and d.

  You can leave those ports empty.

Brocade port usage for controllers in a MetroCluster configuration

The following tables show port usage on Brocade switches. The tables show the maximum supported configuration, with eight controller modules in two DR groups. For smaller configurations, ignore the rows for the additional controller modules. Note that eight ISLs are supported on the Brocade 6510 and G620 switches.

> Port usage for the Brocade 6505 switch in an eight-node MetroCluster configuration is not shown. Due to the limited number of ports, port assignments must be made on a site-by-site basis depending on the controller module model and the number of ISLs and bridge pairs in use.

The following table shows the cabling for the first DR group:

		Brocade 6520, 6510, 6505, G620, G610, or 7840 switch	
Component	**Port**	**Switch 1**	**Switch 2**

controller_x_1	FC-VI port a	0	
	FC-VI port b	-	0
	FC-VI port c	1	-
	FC-VI port d	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3
controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	FC-VI port c	5	-
	FC-VI port d	-	5
	HBA port a	6	-
	HBA port b	-	6
	HBA port c	7	-
	HBA port d	-	7

The following table shows the cabling for the second DR group:

		Brocade 6510		**Brocade 6520**		**Brocade G620**	
Component	**Port**	**Switch 1**	**Switch 2**	**Switch 1**	**Switch 2**	**Switch 1**	**Switch 2**

controller_x_3	FC-VI port a	24	-	48	-	18	-
	FC-VI port b	-	24	-	48	-	18
	FC-VI port c	25	-	49	-	19	-
	FC-VI port d	-	25	-	49	-	19
	HBA port a	26	-	50	-	24	-
	HBA port b	-	26	-	50	-	24
	HBA port c	27	-	51	-	25	-
	HBA port d	-	27	-	51	-	25
controller_x_4	FC-VI port a	28	-	52	-	22	-
	FC-VI port b	-	28	-	52	-	22
	FC-VI port c	29	-	53	-	23	-
	FC-VI port d	-	29	-	53	-	23
	HBA port a	30	-	54	-	28	-
	HBA port b	-	30	-	54	-	28
	HBA port c	31	-	55	-	29	-
	HBA port d	-	31	-	55	-	29
ISLs							
ISL 1		40	40	23	23	40	40
ISL 2		41	41	47	47	41	41
ISL 3		42	42	71	71	42	42
ISL 4		43	43	95	95	43	43

ISL 5	44	44	Not supported	44	44
ISL 6	45	45		45	45
ISL 7	46	46		46	46
ISL 8	47	47		47	47

Cisco port usage for controllers in a MetroCluster configuration running ONTAP 9.4 or later

The tables show the maximum supported configuration, with eight controller modules in two DR groups. For smaller configurations, ignore the rows for the additional controller modules.

Cisco 9396S port usage

Cisco 9396S			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8
controller_x_3	FC-VI port a	49	
	FC-VI port b	-	49
	FC-VI port c	50	
	FC-VI port d	-	50
	HBA port a	51	
	HBA port b	-	51
	HBA port c	52	
	HBA port d	-	52

controller_x_4	FC-VI port a	53	-
	FC-VI port b	-	53
	FC-VI port c	54	-
	FC-VI port d	-	54
	HBA port a	55	-
	HBA port b	-	55
	HBA port c	56	-
	HBA port d	-	56

Cisco 9148S port usage

Cisco 9148S			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8
controller_x_3	FC-VI port a	25	
	FC-VI port b	-	25
	FC-VI port c	26	-
	FC-VI port d	-	26
	HBA port a	27	-
	HBA port b	-	27
	HBA port c	28	-
	HBA port d	-	28

controller_x_4	FC-VI port a	29	-
	FC-VI port b	-	29
	FC-VI port c	30	-
	FC-VI port d	-	30
	HBA port a	31	-
	HBA port b	-	31
	HBA port c	32	-
	HBA port d	-	32

Cisco 9132T port usage

Cisco 9132T			
MDS module 1			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8
MDS module 2			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_3	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_4	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8

Cisco 9250 port usage

> The following table shows systems with two FC-VI ports. AFF A700 and FAS9000 systems have four FC-VI ports (a, b, c, and d). If using an AFF A700 or FAS9000 system, the port assignments move along by one position. For example, FC-VI ports c and d go to switch port 2 and HBA ports a and b go to switch port 3.

Cisco 9250i			
The Cisco 9250i switch is not supported for eight-node MetroCluster configurations.			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3

controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	HBA port a	5	-
	HBA port b	-	5
	HBA port c	6	-
	HBA port d	-	6
controller_x_3	FC-VI port a	7	-
	FC-VI port b	-	7
	HBA port a	8	-
	HBA port b	-	8
	HBA port c	9	-
	HBA port d	-	9
controller_x_4	FC-VI port a	10	-
	FC-VI port b	-	10
	HBA port a	11	-
	HBA port b	-	11
	HBA port c	13	-
	HBA port d	-	13

Shared initiator and shared target support for MetroCluster configuration with array LUNs

Being able to share a given FC initiator port or target ports is useful for organizations that want to minimize the number of initiator or target ports used. For example, an organization that expects low I/O usage over an FC initiator port or target ports might prefer to share FC initiator port or target ports instead of dedicating each FC initiator port to a single target port.

However sharing of initiator or target ports can adversely affect performance.

How to support Shared Initiator and Shared Target configuration with Array LUNs in a MetroCluster environment

Cabling the FC-VI and HBA ports in a MetroCluster configuration with array LUNs

For a fabric-attached MetroCluster configuration with array LUNs, you must connect the controllers in a MetroCluster configuration to the storage arrays through FC switches.

Cabling the FC-VI and HBA ports in a two-node fabric-attached MetroCluster configuration with array LUNs

If you are setting up a two-node fabric-attached MetroCluster configuration with array LUNs, you must cable the FC-VI ports and the HBA ports to the switch ports.

About this task

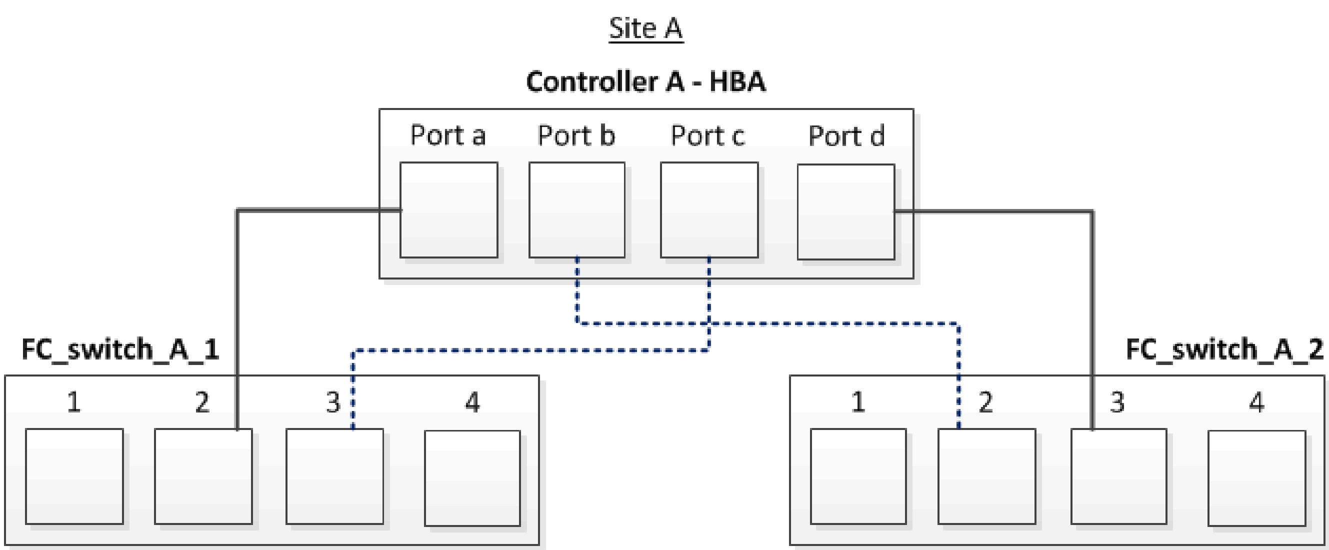
- You must repeat this task for each controller at both of the MetroCluster sites.
- If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the HBA ports and switch ports specified for configuration with disks.
  - Port assignments for FC switches when using ONTAP 9.1 and later
  - Port assignments for FC switches when using ONTAP 9.0

Steps

1. Cable the FC-VI ports from the controller to alternate switch ports.
2. Perform the controller-to-switch cabling at both of the MetroCluster sites.

   You must ensure redundancy in connections from the controller to the switches. Therefore, for each controller at a site, you must ensure that both of the HBA ports in the same port pair are connected to alternate FC switches.

   The following example shows the connections between the HBA ports on Controller A and ports on FC_switch_A_1 and FC_switch_A_2:



   The following table lists the connections between the HBA ports and the FC switch ports in the illustration:

HBA ports	Switch ports
Port pair	

Port a	FC_switch_A_1, Port 2
Port d	FC_switch_A_2, Port 3
Port pair	
Port b	FC_switch_A_2, Port 2
Port c	FC_switch_A_1, Port 3

After you finish

You should cable the ISLs between the FC switches across the MetroCluster sites.

Cabling the FC-VI and HBA ports in a four-node fabric-attached MetroCluster configuration with array LUNs

If you are setting up a four-node fabric-attached MetroCluster configuration with array LUNs, you must cable the FC-VI ports and the HBA ports to the switch ports.

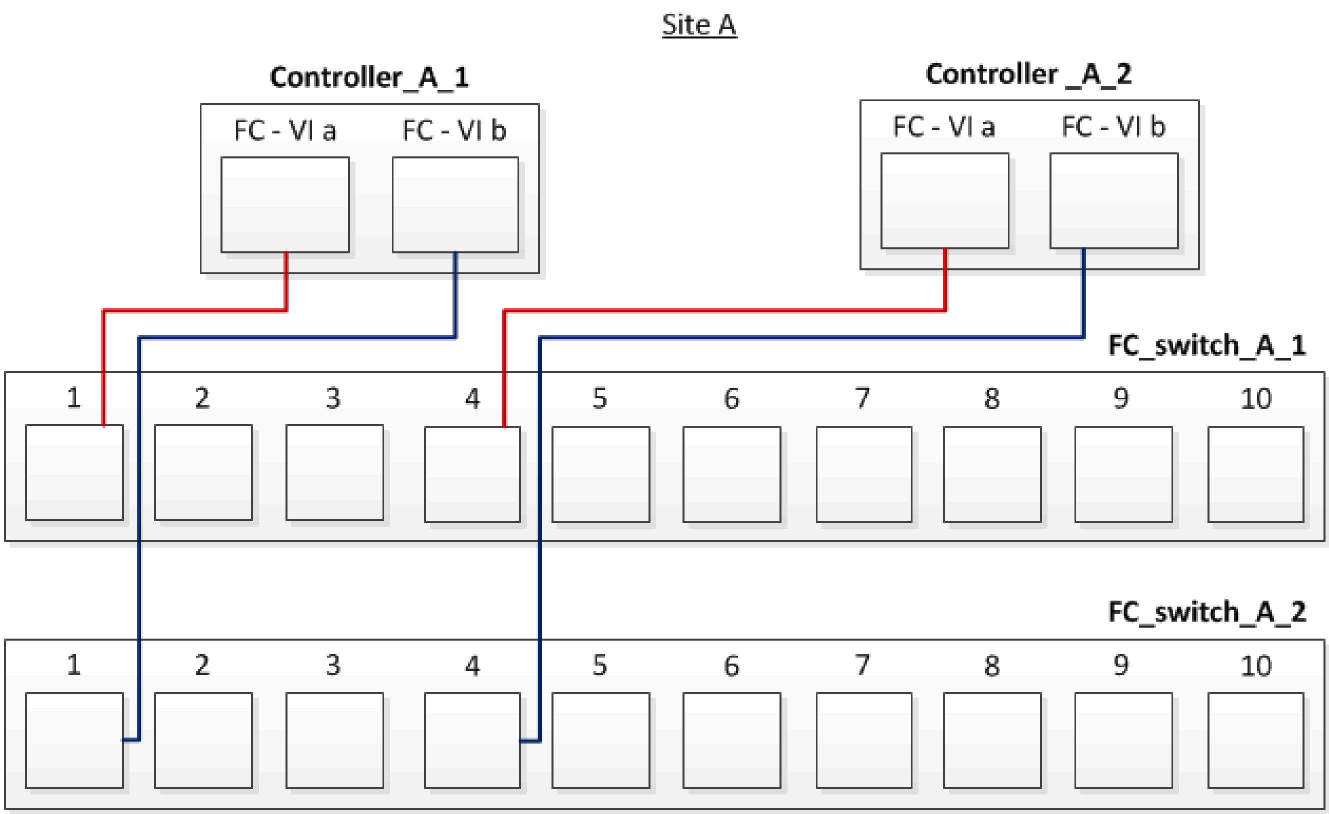
About this task

- You must repeat this task for each controller at both of the MetroCluster sites.
- If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the HBA ports and switch ports specified for configuration with disks.
  - Port assignments for FC switches when using ONTAP 9.1 and later
  - Port assignments for FC switches when using ONTAP 9.0

Steps

1. Cable the FC-VI ports from each controller to the ports on alternate FC switches.

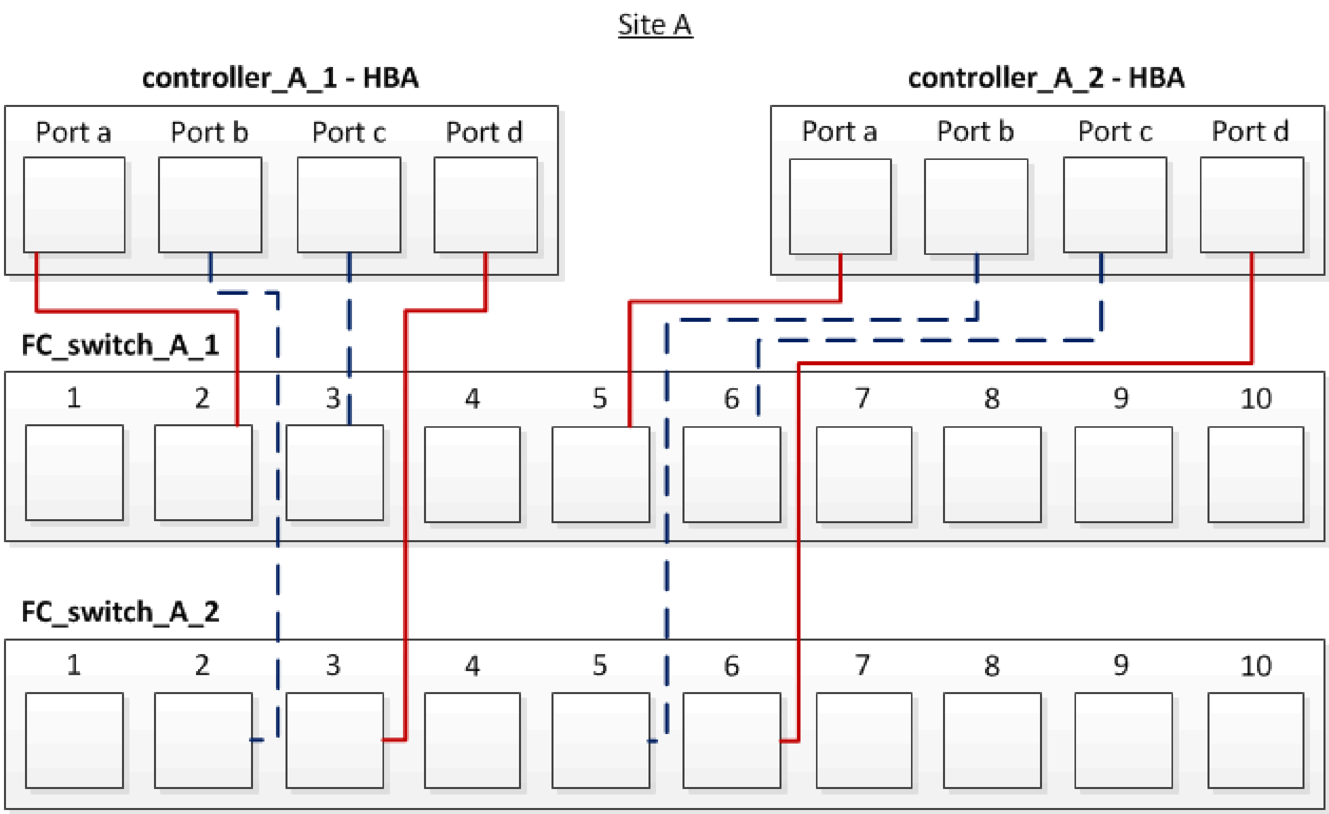
   The following example shows the connections between the FC-VI ports and switch ports at Site A:



2. Perform the controller-to-switch cabling at both of the MetroCluster sites.

   You must ensure redundancy in connections from the controller to the switches. Therefore, for each controller at a site, you must ensure that both of the HBA ports in the same port pair are connected to alternate FC switches.

   The following example shows the connections between the HBA ports and switch ports at Site A:



The following table lists the connections between the HBA ports on controller_A_1 and the FC switch ports in the illustration:

HBA ports	Switch ports
Port pair	
Port a	FC_switch_A_1, Port 2
Port d	FC_switch_A_2, Port 3
Port pair	
Port b	FC_switch_A_2, Port 2
Port c	FC_switch_A_1, Port 3

The following table lists the connections between the HBA ports on controller_A_2 and the FC switch ports in the illustration:

HBA ports	Switch ports
Port pair	
Port a	FC_switch_A_1, Port 5
Port d	FC_switch_A_2, Port 6

Port pair	
Port b	FC_switch_A_2, Port 5
Port c	FC_switch_A_1, Port 6

After you finish

You should cable the ISLs between the FC switches across the MetroCluster sites.

Related information

When you are connecting ONTAP systems to FC switches for setting up a MetroCluster configuration with array LUNs, you must connect FC-VI and HBA ports from each controller to specific switch ports.

Switch ports required for a MetroCluster configuration with array LUNs

Cabling the FC-VI and HBA ports in an eight-node fabric-attached MetroCluster configuration with array LUNs

If you are setting up an eight-node fabric-attached MetroCluster configuration with array LUNs, you must cable the FC-VI ports and the HBA ports to the switch ports.

About this task

- You must repeat this task for each controller at both of the MetroCluster sites.
- If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the HBA ports and switch ports specified for configuration with disks.
  - Port assignments for FC switches when using ONTAP 9.1 and later
  - Port assignments for FC switches when using ONTAP 9.0

Step

1. Cable the FC-VI ports and HBA ports from each controller to the ports on alternate FC switches. Refer to the following tables:

Cabling configurations for FibreBridge 7500N or 7600N using both FC ports

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)				
MetroCluster 1 or DR Group 1				
Component	**Port**	**Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1, and DCX 8510-8**		**Brocade switch G720**
		Connects to FC_switch…	**Connects to switch port…**	**Connects to switch port…**

controller_x_1		FC-VI port a	1	0	0
		FC-VI port b	2	0	0
		FC-VI port c	1	1	1
		FC-VI port d	2	1	1
		HBA port a	1	2	8
		HBA port b	2	2	8
		HBA port c	1	3	9
		HBA port d	2	3	9
controller_x_2		FC-VI port a	1	4	4
		FC-VI port b	2	4	4
		FC-VI port c	1	5	5
		FC-VI port d	2	5	5
		HBA port a	1	6	12
		HBA port b	2	6	12
		HBA port c	1	7	13
		HBA port d	2	7	13
Stack 1	bridge_x_1a	FC1	1	8	10
		FC2	2	8	10
	bridge_x_1B	FC1	1	9	11
		FC2	2	9	11

Stack 2	bridge_x_2a	FC1	1	10	14
		FC2	2	10	14
	bridge_x_2B	FC1	1	11	15
		FC2	2	11	15
Stack 3	bridge_x_3a	FC1	1	12*	16
		FC2	2	12*	16
	bridge_x_3B	FC1	1	13*	17
		FC2	2	13*	17
Stack y	bridge_x_ya	FC1	1	14*	20
		FC2	2	14*	20
	bridge_x_yb	FC1	1	15*	21
		FC2	2	15*	21
*** Ports 12 through 15 are reserved for the second MetroCluster or DR group on the Brocade 7840 switch.**					
Note: Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620, G630, G620-1 and G630-1 switches.					

After you finish

You should cable the ISLs between the FC switches across the MetroCluster sites.

Cabling configurations for Cisco 9250i

Cisco 9250i*			
Component	**Port**	**Switch 1**	**Switch 2**

controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3
controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	HBA port a	5	-
	HBA port b	-	5
	HBA port c	6	-
	HBA port d	-	6
controller_x_3	FC-VI port a	7	-
	FC-VI port b	-	7
	HBA port a	8	-
	HBA port b	-	8
	HBA port c	9	-
	HBA port d	-	9

controller_x_4	FC-VI port a	10	-
	FC-VI port b	-	10
	HBA port a	11	-
	HBA port b	-	11
	HBA port c	13	-
	HBA port d	-	13

After you finish

You should cable the ISLs between the FC switches across the MetroCluster sites.

Cabling the ISLs in a MetroCluster configuration with array LUNs

You must connect the FC switches across the sites through Inter-Switch Links (ISLs) to form switch fabrics in your MetroCluster configuration with array LUNs.

Steps

1. Connect the switches at each site to the ISL or ISLs, using the cabling in the table that corresponds to your configuration and switch model.

   The switch port numbers that you can use for the FC ISLs are as follows:

Switch model	ISL port	Switch port
Brocade 6520	ISL port 1	23
	ISL port 2	47
	ISL port 3	71
	ISL port 4	95
Brocade 6505	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23

Brocade 6510 and Brocade DCX 8510-8	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47
Brocade 7810	ISL port 1	ge2 (10-Gbps)
	ISL port 2	ge3(10-Gbps)
	ISL port 3	ge4 (10-Gbps)
	ISL port 4	ge5 (10-Gbps)
	ISL port 5	ge6 (10-Gbps)
	ISL port 6	ge7 (10-Gbps)
Brocade 7840 **Note**: The Brocade 7840 switch supports either two 40 Gbps VE-ports or up to four 10 Gbps VE-ports per switch for the creation of FCIP ISLs.	ISL port 1	ge0 (40-Gbps) or ge2 (10-Gbps)
	ISL port 2	ge1 (40-Gbps) or ge3 (10-Gbps)
	ISL port 3	ge10 (10-Gbps)
	ISL port 4	ge11 (10-Gbps)
Brocade G610	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23

Brocade G620, G620-1, G630, G630-1, G720	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47

Switch mode l	**ISL port**	**Switch port**
Cisco 9396S	ISL 1	44
	ISL 2	48
	ISL 3	92
	ISL 4	96
Cisco 9250i with 24 port license	ISL 1	12
	ISL 2	16
	ISL 3	20
	ISL 4	24
Cisco 9148S	ISL 1	20
	ISL 2	24
	ISL 3	44
	ISL 4	48

Cisco 9132T	ISL 1	MDS module 1 port 13
	ISL 2	MDS module 1 port 14
	ISL 3	MDS module 1 port 15
	ISL 4	MDS module 1 port 16
*** The Cisco 9250i switch uses the FCIP ports for the ISL. There are certain limitations and procedures for using the FCIP ports.**		
Ports 40 through 48 are 10 GbE ports and are not used in the MetroCluster configuration.		

Cabling the cluster interconnect in eight- or four-node configurations

In eight- or four-node MetroCluster configurations, you must cable the cluster interconnect between the local controller modules at each site.

About this task

This task is not required on two-node MetroCluster configurations.

This task must be performed at both MetroCluster sites.

Step

1. Cable the cluster interconnect from one controller module to the other, or if cluster interconnect switches are used, from each controller module to the switches.

Related information

AFF and FAS Documentation Center

Network and LIF management

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.

Related information

Cluster and SVM peering express configuration

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.

Considerations for configuring cluster peering

Cabling the HA interconnect

If you have an eight- or a four-node MetroCluster configuration and the storage controllers within the HA pairs are in separate chassis, you must cable the HA interconnect between the controllers.

About this task

- This task does not apply to two-node MetroCluster configurations.
- This task must be performed at both MetroCluster sites.
- The HA interconnect must be cabled only if the storage controllers within the HA pair are in separate chassis.

  Some storage controller models support two controllers in a single chassis, in which case they use an internal HA interconnect.

Steps

1. Cable the HA interconnect if the storage controller's HA partner is in a separate chassis.

   AFF and FAS Documentation Center

2. If the MetroCluster site includes two HA pairs, repeat the previous steps on the second HA pair.
3. Repeat this task at the MetroCluster partner site.

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 storage arrays to FC switches in a MetroCluster configuration

You must connect storage arrays to FC switches so that the ONTAP systems in the MetroCluster configuration can access a specific array LUN through at least two paths.

Before you begin

- The storage arrays must be set up to present array LUNs to ONTAP.
- The ONTAP controllers must be connected to the FC switches.
- The ISLs must be cabled between the FC switches across the MetroCluster sites.
- You must repeat this task for each storage array at both of the MetroCluster sites.
- You must connect the controllers in a MetroCluster configuration to the storage arrays through FC switches.

Steps

1. Connect the storage array ports to FC switch ports.

   At each site, connect the redundant port pairs in the storage array to FC switches on alternate fabrics. This provides redundancy in the paths for accessing the array LUNs.

Related information

- Configuring switch zoning enables you to define which array LUNs can be viewed by a specific ONTAP system in the MetroCluster configuration.

  Switch zoning in a MetroCluster configuration with array LUNs

- In a MetroCluster configuration with array LUNs, you must connect the storage array ports that form a redundant port pair to alternate FC switches.

  Example of cabling storage array ports to FC switches in a two-node MetroCluster configuration

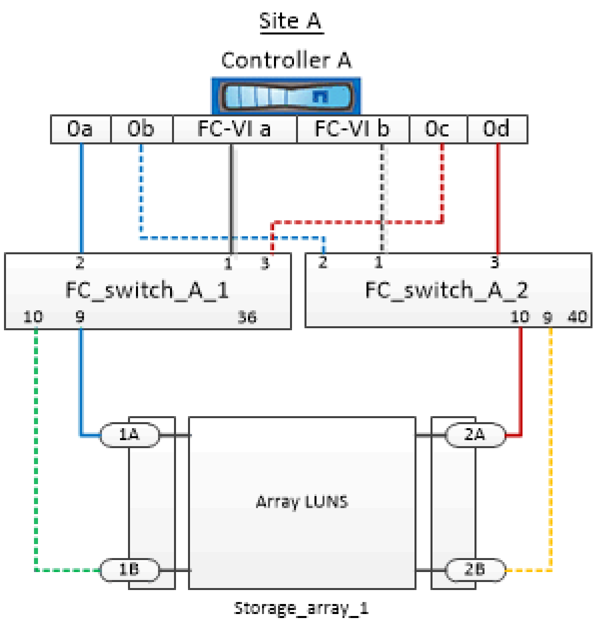
  Example of cabling storage array ports to FC switches in a four-node MetroCluster configuration

  Example of cabling storage array ports to FC switches in an eight-node MetroCluster configuration

Example of cabling storage array ports to FC switches in a two-node MetroCluster configuration

In a MetroCluster configuration with array LUNs, you must connect the storage array ports that form a redundant port pair to alternate FC switches.

The following illustration shows the connections between storage arrays and FC switches in a two-node fabric-attached MetroCluster configuration with array LUNs:



The connections between storage array ports and FC switch ports are similar for both stretch and fabric-attached variants of two-node MetroCluster configurations with array LUNs.

If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the switch ports specified for the configuration with disks.

Port assignments for FC switches when using ONTAP 9.1 and later

In the illustration, the redundant array port pairs for both the sites are as follows:

- Storage array at Site A:
  - Ports 1A and 2A
  - Ports 1B and 2B
- Storage array at Site B:
  - Ports 1A' and 2A'
  - Ports 1B' and 2B'

FC_switch_A_1 at Site A and FC_switch_B_1 at Site B are connected to form fabric_1. Similarly, FC_switch_A_2 at Site A and FC_switch_B_2 are connected to form fabric_2.

The following table lists the connections between the storage array ports and the FC switches for the example MetroCluster illustration:

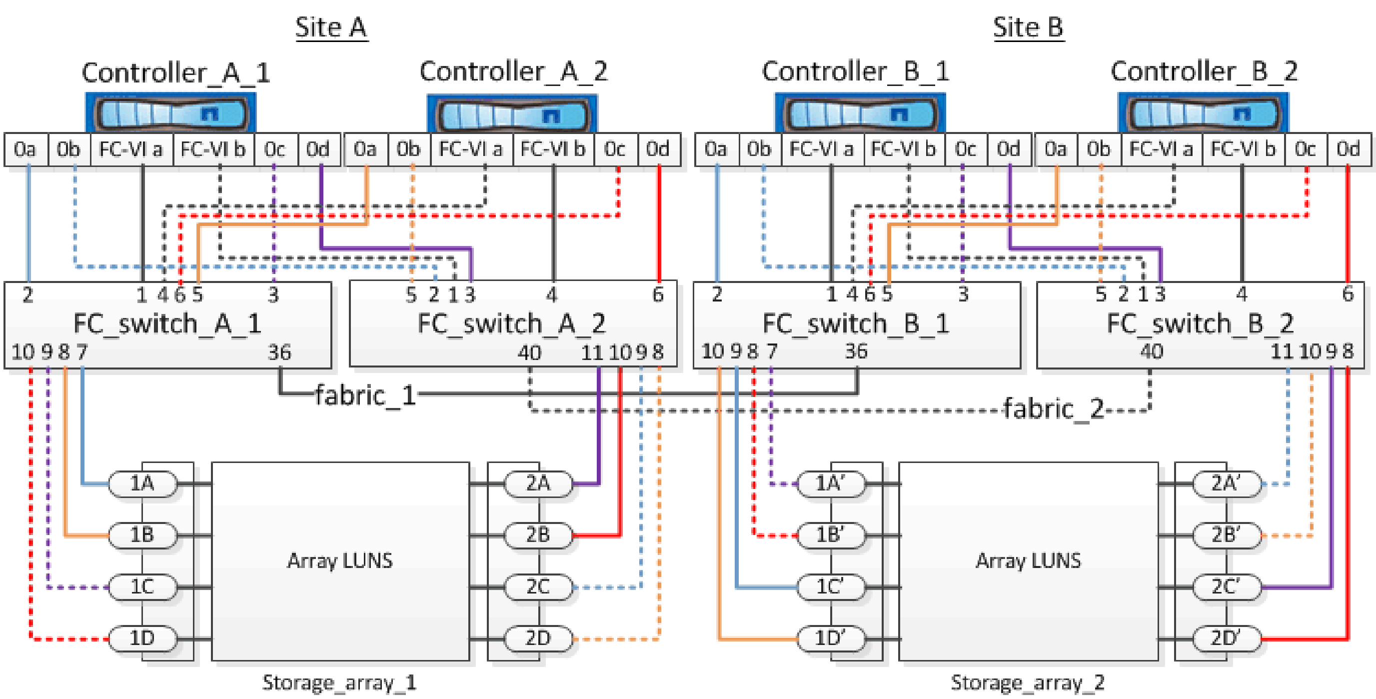
Array LUN ports	FC switch ports	Switch fabrics
	Site A	
1A	FC_switch_A_1, Port 9	fabric_1
2A	FC_switch_A_2, Port 10	fabric_2
1B	FC_switch_A_1, Port 10	fabric_1

2B	FC_switch_A_2, Port 9	fabric_2
Site B		
1A'	FC_switch_B_1, Port 9	fabric_1
2A'	FC_switch_B_2, Port 10	fabric_2
1B'	FC_switch_B_1, Port 10	fabric_1
2B'	FC_switch_B_2, Port 9	fabric_2

Example of cabling storage array ports to FC switches in a four-node MetroCluster configuration

In a MetroCluster configuration with array LUNs, you must connect the storage array ports that form a redundant port pair to alternate FC switches.

The following reference illustration shows the connections between storage arrays and FC switches in a four-node MetroCluster configuration with array LUNs:



If you plan to use disks in addition to array LUNs in your MetroCluster configuration, you must use the switch ports specified for the configuration with disks.

Port assignments for FC switches when using ONTAP 9.1 and later

In the illustration, the redundant array port pairs for both the sites are as follows:

- Storage array at Site A:
  - Ports 1A and 2A

    ◦ Ports 1B and 2B
    ◦ Ports 1C and 2C
    ◦ Ports 1D and 2D
* Storage array at Site B:
    ◦ Ports 1A' and 2A'
    ◦ Ports 1B' and 2B'
    ◦ Ports 1C' and 2C'
    ◦ Ports 1D' and 2D'

FC_switch_A_1 at Site A and FC_switch_B_1 at Site B are connected to form fabric_1. Similarly, FC_switch_A_2 at Site A and FC_switch_B_2 are connected to form fabric_2.

The following table lists the connections between the storage array ports and the FC switches for the MetroCluster illustration:

Array LUN ports	FC switch ports	Switch fabrics
Site A		
1A	FC_switch_A_1, Port 7	fabric_1
2A	FC_switch_A_2, Port 11	fabric_2
1B	FC_switch_A_1, Port 8	fabric_1
2B	FC_switch_A_2, Port 10	fabric_2
1C	FC_switch_A_1, Port 9	fabric_1
2C	FC_switch_A_2, Port 9	fabric_2
1D	FC_switch_A_1, Port 10	fabric_1
2D	FC_switch_A_2, Port 8	fabric_2
Site B		
1A'	FC_switch_B_1, Port 7	fabric_1
2A'	FC_switch_B_2, Port 11	fabric_2
1B'	FC_switch_B_1, Port 8	fabric_1
2B'	FC_switch_B_2, Port 10	fabric_2
1C'	FC_switch_B_1, Port 9	fabric_1

2C'	FC_switch_B_2, Port 9	fabric_2
1D'	FC_switch_B_1, Port 10	fabric_1
2D'	FC_switch_B_2, Port 8	fabric_2

Example of cabling storage array ports to FC switches in an eight-node MetroCluster configuration

In a MetroCluster configuration with array LUNs, you must connect the storage array ports that form a redundant port pair to alternate FC switches.

An eight-node MetroCluster configuration consists of two four-node DR groups. The first DR group consists of the following nodes:

- controller_A_1
- controller_A_2
- controller_B_1
- controller_B_2

The second DR group consists of the following nodes:

- controller_A_3
- controller_A_4
- controller_B_3
- controller_B_4

To cable the array ports for the first DR group, you can use the cabling examples for a four-node MetroCluster configuration for the first DR group.

Example of cabling storage array ports to FC switches in a four-node MetroCluster configuration

To cable the array ports for the second DR group, follow the same examples and extrapolate for the FC-VI ports and FC initiator ports belonging to the controllers in the second DR group.

Switch zoning in a MetroCluster configuration with array LUNs

Configuring switch zoning enables you to define which array LUNs can be viewed by a specific ONTAP system in the MetroCluster configuration.

Related information

Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by specific ONTAP systems.

Example of switch zoning in a two-node MetroCluster configuration with array LUNs

Example of switch zoning in a four-node MetroCluster configuration with array LUNs

Example of switch zoning in an eight-node MetroCluster configuration with array LUNs

Requirements for switch zoning in a MetroCluster configuration with array LUNs

When using switch zoning in a MetroCluster configuration with array LUNs, you must ensure that certain basic requirements are followed.

The requirements for switch zoning in a MetroCluster configuration with array LUNs are as follows:

- The MetroCluster configuration must follow the single-initiator to single-target zoning scheme.

  Single-initiator to single-target zoning limits each zone to a single FC initiator port and a single target port.

- The FC-VI ports must be zoned end-to-end across the fabric.
- Sharing of multiple initiator ports with a single target port can cause performance issues.

  Similarly, sharing of multiple target ports with a single initiator port can cause performance issues.

- You must have performed a basic configuration of the FC switches used in the MetroCluster configuration.

  Configuring the Cisco or Brocade FC switches manually

Shared initiator and shared target support for MetroCluster configuration with array LUNs

Being able to share a given FC initiator port or target ports is useful for organizations that want to minimize the number of initiator or target ports used. For example, an organization that expects low I/O usage over an FC initiator port or target ports might prefer to share FC initiator port or target ports instead of dedicating each FC initiator port to a single target port.

However sharing of initiator or target ports can adversely affect performance.

Related information

How to support Shared Initiator and Shared Target configuration with Array LUNs in a MetroCluster environment

- Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by specific ONTAP systems.

  Example of switch zoning in a two-node MetroCluster configuration with array LUNs

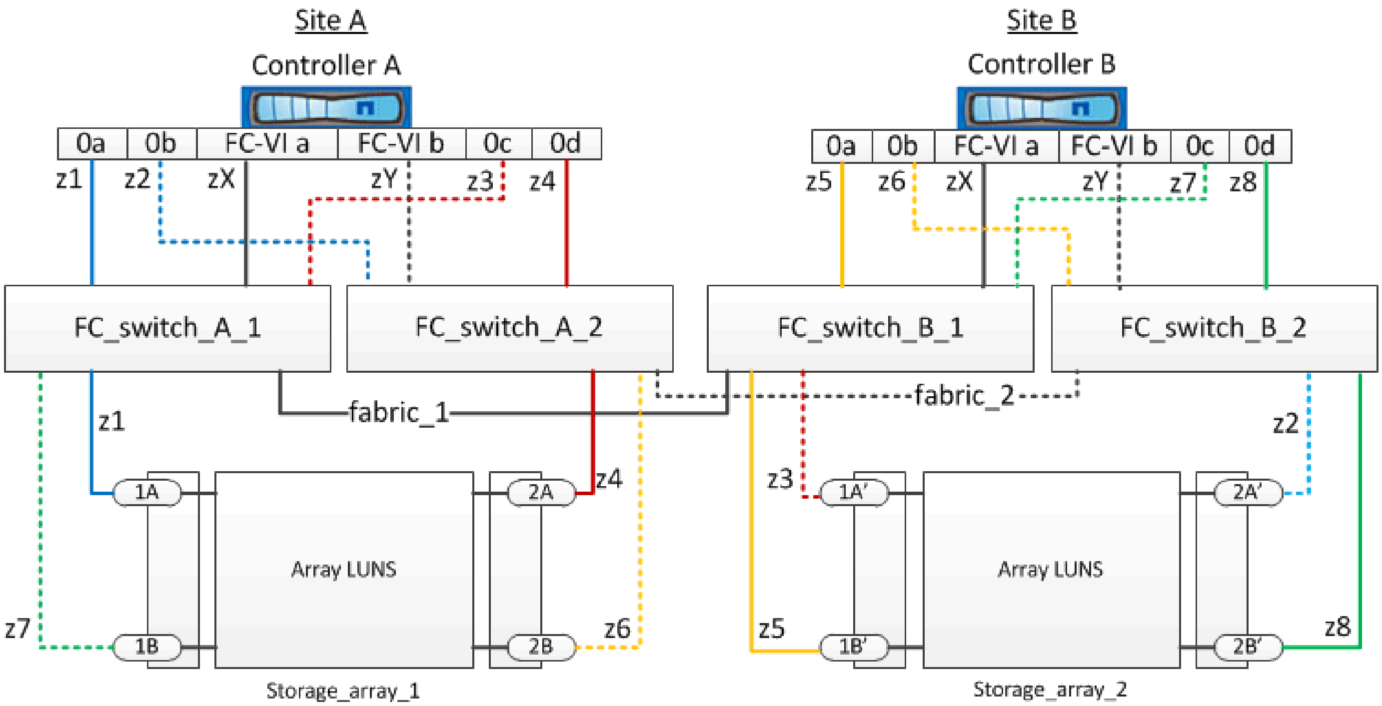
  Example of switch zoning in a four-node MetroCluster configuration with array LUNs

  Example of switch zoning in an eight-node MetroCluster configuration with array LUNs

Example of switch zoning in a two-node MetroCluster configuration with array LUNs

Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by specific ONTAP systems.

You can use the following example as a reference when determining zoning for a two-node fabric-attached MetroCluster configuration with array LUNs:



The example shows single-initiator to single-target zoning for the MetroCluster configurations. The lines in the example represent zones rather than connections; each line is labeled with its zone number.

In the example, array LUNs are allocated on each storage array. LUNs of equal size are provisioned on the storage arrays at both sites, which is a SyncMirror requirement. Each ONTAP system has two paths to array LUNs. The ports on the storage array are redundant.

The redundant array port pairs for both the sites are as follows:

- Storage array at Site A:
  - Ports 1A and 2A
  - Ports 1B and 2B
- Storage array at Site B:
  - Ports 1A' and 2A'
  - Ports 1B' and 2B'

The redundant port pairs on each storage array form alternate paths. Therefore, both the ports of the port pairs can access the LUNs on the respective storage arrays.

The following table shows the zones for the illustrations:

Zone	ONTAP controller and initiator port	Storage array port
FC_switch_A_1		
z1	Controller A: Port 0a	Port 1A
z3	Controller A: Port 0c	Port 1A'

FC_switch_A_2		
z2	Controller A: Port 0b	Port 2A'
z4	Controller A: Port 0d	Port 2A
FC_switch_B_1		
z5	Controller B: Port 0a	Port 1B'
z7	Controller B: Port 0c	Port 1B
FC_switch_B_2		
z6	Controller B: Port 0b	Port 2B
z8	Controller B: Port 0d	Port 2B'

The following table shows the zones for the FC-VI connections:

Zone	ONTAP controller and initiator port	Switch
Site A		
zX	Controller A: Port FC-VI a	FC_switch_A_1
zY	Controller A: Port FC-VI b	FC_switch_A_2
Site B		
zX	Controller B: Port FC-VI a	FC_switch_B_1
zY	Controller B: Port FC-VI b	FC_switch_B_2

Related information

- Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by a specific ONTAP system.

  Requirements for switch zoning in a MetroCluster configuration with array LUNs

  Example of switch zoning in a four-node MetroCluster configuration with array LUNs

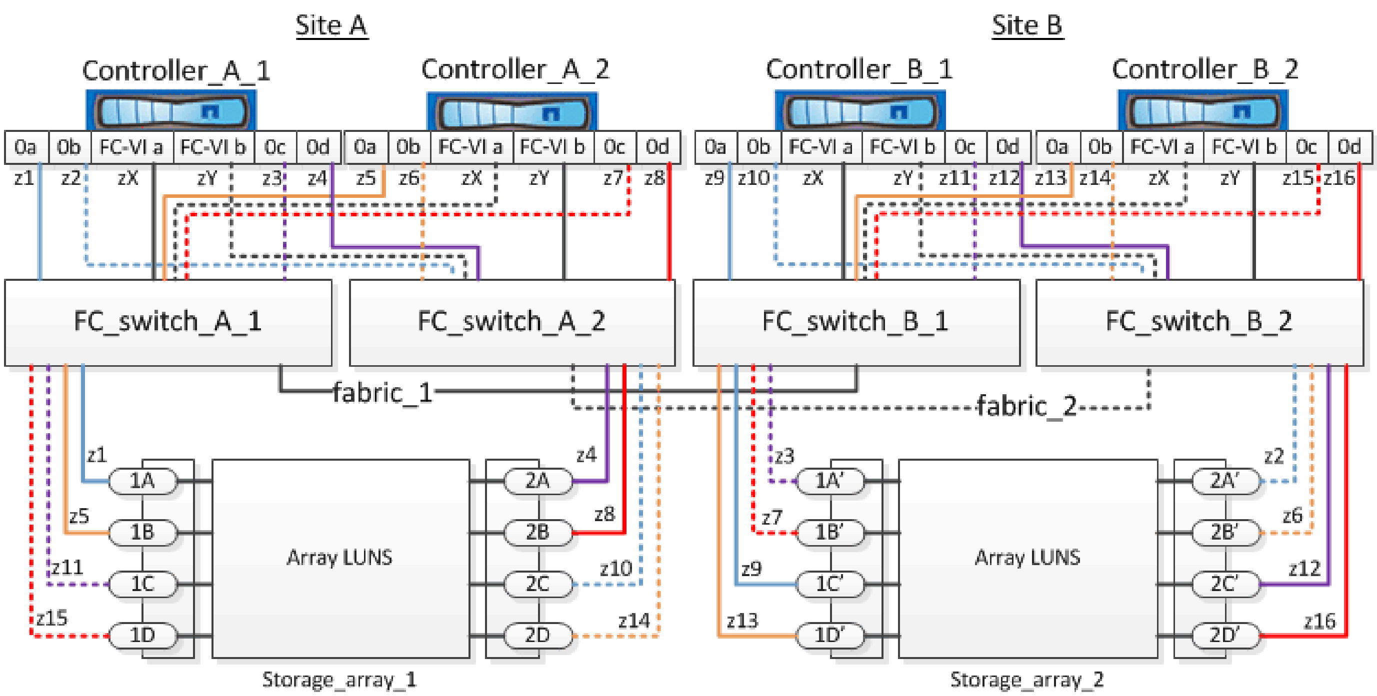
- When using switch zoning in a MetroCluster configuration with array LUNs, youmust ensure that certain basic requirements are followed.

  Example of switch zoning in an eight-node MetroCluster configuration with array LUNs

Example of switch zoning in a four-node MetroCluster configuration with array LUNs

Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by a specific ONTAP systems.

You can use the following example as a reference when determining zoning for a four-node MetroCluster configuration with array LUNs. The example shows single-initiator to single-target zoning for a MetroCluster configuration. The lines in the following example represent zones rather than connections; each line is labeled with its zone number:



In the illustration, array LUNs are allocated on each storage array for the MetroCluster configuration. LUNs of equal size are provisioned on the storage arrays at both sites, which is a SyncMirror requirement. Each ONTAP system has two paths to array LUNs. The ports on the storage array are redundant.

In the illustration, the redundant array port pairs for both the sites are as follows:

- Storage array at Site A:
  - Ports 1A and 2A
  - Ports 1B and 2B
  - Ports 1C and 2C
  - Ports 1D and 2D
- Storage array at Site B:
  - Ports 1A' and 2A'
  - Ports 1B' and 2B'
  - Ports 1C' and 2C'
  - Ports 1D' and 2D'

The redundant port pairs on each storage array form alternate paths. Therefore, both the ports of the port pairs can access the LUNs on the respective storage arrays.

The following tables show the zones for this example:

Zones for FC_switch_A_1

Zone	ONTAP controller and initiator port	Storage array port
z1	Controller_A_1: Port 0a	Port 1A
z3	Controller_A_1: Port 0c	Port 1A'
z5	Controller_A_2: Port 0a	Port 1B
z7	Controller_A_2: Port 0c	Port 1B'

Zones for FC_switch_A_2

Zone	ONTAP controller and initiator port	Storage array port
z2	Controller_A_1: Port 0b	Port 2A'
z4	Controller_A_1: Port 0d	Port 2A
z6	Controller_A_2: Port 0b	Port 2B'
z8	Controller_A_2: Port 0d	Port 2B

Zones for FC_switch_B_1

Zone	ONTAP controller and initiator port	Storage array port
z9	Controller_B_1: Port 0a	Port 1C'
z11	Controller_B_1: Port 0c	Port 1C
z13	Controller_B_2: Port 0a	Port 1D'
z15	Controller_B_2: Port 0c	Port 1D

Zones for FC_switch_B_2

Zone	ONTAP controller and initiator port	Storage array port
z10	Controller_B_1: Port 0b	Port 2C

z12	Controller_B_1: Port 0d	Port 2C'
z14	Controller_B_2: Port 0b	Port 2D
z16	Controller_B_2: Port 0d	Port 2D'

Zones for the FC-VI connections at Site A

Zone	ONTAP controller and FC initiator port	Switch
zX	Controller_A_1: Port FC-VI a	FC_switch_A_1
zY	Controller_A_1: Port FC-VI b	FC_switch_A_2
zX	Controller_A_2: Port FC-VI a	FC_switch_A_1
zY	Controller_A_2: Port FC-VI b	FC_switch_A_2

Zones for the FC-VI connections at Site B

Zone	ONTAP controller and FC initiator port	Switch
zX	Controller_B_1: Port FC-VI a	FC_switch_B_1
zY	Controller_B_1: Port FC-VI b	FC_switch_B_2
zX	Controller_B_2: Port FC-VI a	FC_switch_B_1
zY	Controller_B_2: Port FC-VI b	FC_switch_B_2

Related information

- Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by specific ONTAP systems.

  Example of switch zoning in a two-node MetroCluster configuration with array LUNs

  Example of switch zoning in an eight-node MetroCluster configuration with array LUNs

- When using switch zoning in a MetroCluster configuration with array LUNs, you must ensure that certain basic requirements are followed.

  Requirements for switch zoning in a MetroCluster configuration with array LUNs

Example of switch zoning in an eight-node MetroCluster configuration with array LUNs

Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by specific ONTAP systems.

An eight-node MetroCluster configuration consists of two four-node DR groups. The first DR group consists of the following nodes:

- controller_A_1
- controller_A_2
- controller_B_1
- controller_B_2

The second DR group consists of the following nodes:

- controller_A_3
- controller_A_4
- controller_B_3
- controller_B_4

To configure the switch zoning, you can use the zoning examples for a four-node MetroCluster configuration for the first DR group.

Example of switch zoning in a four-node MetroCluster configuration with array LUNs

To configure zoning for the second DR group, follow the same examples and requirements for the FC initiator ports and array LUNs belonging to the controllers in the second DR group.

Related information

- Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by specific ONTAP systems.

  Example of switch zoning in a two-node MetroCluster configuration with array LUNs

  Example of switch zoning in a four-node MetroCluster configuration with array LUNs

- When using switch zoning in a MetroCluster configuration with array LUNs, you must ensure that certain basic requirements are followed.

  Requirements for switch zoning in a MetroCluster configuration with array LUNs

Setting up ONTAP in a MetroCluster configuration with array LUNs

After connecting the devices in the MetroCluster configuration, you must set up the ONTAP systems to use the storage on the storage array. You must also configure any required ONTAP feature.

Verifying and configuring the HA state of components in Maintenance mode

When configuring a storage system in a MetroCluster configuration, you must make sure that the high-availability (HA) state of the controller module and chassis components is "mcc" or "mcc-2n" so that these components boot properly.

Before you begin

The system must be in Maintenance mode.

About this task

This task is not required on systems that are received from the factory.

Steps

1. In Maintenance mode, display the HA state of the controller module and chassis:

   `ha-config show`

   The correct HA state depends on your MetroCluster configuration.

Number of controllers in the MetroCluster configuration	HA state for all components should be…
Eight- or four-node MetroCluster FC configuration	mcc
Two-node MetroCluster FC configuration	mcc-2n
MetroCluster IP configuration	mccip

2. If the displayed system state of the controller is not correct, set the HA state for the controller module:

Number of controllers in the MetroCluster configuration	Command
Eight- or four-node MetroCluster FC configuration	`ha-config modify controller mcc`
Two-node MetroCluster FC configuration	`ha-config modify controller mcc-2n`
MetroCluster IP configuration	`ha-config modify controller mccip`

3. If the displayed system state of the chassis is not correct, set the HA state for the chassis:

Number of controllers in the MetroCluster configuration	Command
Eight- or four-node MetroCluster FC configuration	`ha-config modify chassis mcc`
Two-node MetroCluster FC configuration	`ha-config modify chassis mcc-2n`
MetroCluster IP configuration	`ha-config modify chassis mccip`

4. Boot the node to ONTAP:

   ```
   boot_ontap
   ```

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

Configuring ONTAP on a system that uses only array LUNs

If you want to configure ONTAP for use with array LUNs, you must configure the root aggregate and root volume, reserve space for diagnostics and recovery operations, and set up the cluster.

Before you begin

- The ONTAP system must be connected to the storage array.
- The storage array administrator must have created LUNs and presented them to ONTAP.
- The storage array administrator must have configured the LUN security.

About this task

You must configure each node that you want to use with array LUNs. If the node is in an HA pair, then you must complete the configuration process on one node before proceeding with the configuration on the partner node.

Steps

1. Power on the primary node and interrupt the boot process by pressing Ctrl-C when you see the following message on the console:

   ```
   Press CTRL-C for special boot menu.
   ```

2. Select option **4 (Clean configuration and initialize all disks)** on the boot menu.

   The list of array LUNs made available to ONTAP is displayed. In addition, the array LUN size required for root volume creation is also specified. The size required for root volume creation differs from one ONTAP system to another.

   - If no array LUNs were previously assigned, ONTAP detects and displays the available array LUNs, as shown in the following example:

```
mcc8040-ams1::> disk show  NET-1.6 -instance
                  Disk: NET-1.6
        Container Type: aggregate
            Owner/Home: mcc8040-ams1-01 / mcc8040-ams1-01
               DR Home: -
    Stack ID/Shelf/Bay: -  / -  / -
                   LUN: 0
                 Array: NETAPP_INF_1
                Vendor: NETAPP
                 Model: INF-01-00
         Serial Number: 60080E50004317B4000003B158E35974
                   UID:
60080E50:004317B4:000003B1:58E35974:00000000:00000000:00000000:000000
00:00000000:00000000
                   BPS: 512
         Physical Size: 87.50GB
              Position: data
Checksum Compatibility: block
             Aggregate: eseries
                  Plex: plex0
Paths:
                                LUN  Initiator Side        Target
Side                                                        Link
Controller         Initiator     ID  Switch Port           Switch
Port           Acc Use  Target Port                TPGN    Speed
I/O KB/s          IOPS
------------------ ---------  -----  --------------------
--------------------  --- ---  -----------------------  ------
-------  ------------  ------------
mcc8040-ams1-01    2c             0  mccb6505-ams1:16      mccb6505-
ams1:18      AO  INU  20330080e54317b4              1   4 Gb/S
0             0
mcc8040-ams1-01    2a             0  mccb6505-ams1:17      mccb6505-
ams1:19      ANO RDY  20320080e54317b4              0   4 Gb/S
0             0

Errors:
-
```

- If array LUNs were previously assigned, for example, through the maintenance mode, they are either marked local or partner in the list of the available array LUNs, depending on whether the array LUNs were selected from the node on which you are installing ONTAP or its HA partner:

  In this example, array LUNs with index numbers 3 and 6 are marked "local" because they had been previously assigned from this particular node:

```
*********************************************************************
*
* No disks are owned by this node, but array LUNs are assigned.
*
* You can use the following information to verify connectivity from
*
* HBAs to switch ports.  If the connectivity of HBAs to switch ports
*
* does not match your expectations, configure your SAN and rescan.
*
* You can rescan by entering 'r' at the prompt for selecting
*
* array LUNs below.

*********************************************************************
*
             HBA  HBA WWPN           Switch port      Switch port
WWPN
              ---  --------           -----------
----------------
              0e 500a098001baf8e0  vgbr6510s203:25
20190027f88948dd
              0f 500a098101baf8e0 vgci9710s202:1-17
2011547feeead680
              0g 500a098201baf8e0  vgbr6510s203:27
201b0027f88948dd
              0h 500a098301baf8e0 vgci9710s202:1-18
2012547feeead680


No native disks were detected, but array LUNs were detected.
You will need to select an array LUN to be used to create the root
aggregate and root volume.

The array LUNs visible to the system are listed below.  Select one
array LUN to be used to
create the root aggregate and root volume.  **The root volume
requires 350.0 GB of space.**

 Warning: The contents of the array LUN you select will be erased by
ONTAP prior to their use.

Index  Array LUN Name           Model   Vendor    Size    Owner
Checksum  Serial Number
-----  -----------------------  ------  ------  --------  ------
--------  ------------------------
```

```
    0   vgci9710s202:2-24.0L19   RAID5   DGC     217.3 GB
Block     6006016083402B0048E576D7
    1   vgbr6510s203:30.126L20   RAID5   DGC     217.3 GB
Block     6006016083402B0049E576D7
    2   vgci9710s202:2-24.0L21   RAID5   DGC     217.3 GB
Block     6006016083402B004AE576D7
    3   vgbr6510s203:30.126L22   RAID5   DGC     405.4 GB  local
Block     6006016083402B004BE576D7
    4   vgci9710s202:2-24.0L23   RAID5   DGC     217.3 GB
Block     6006016083402B004CE576D7
    5   vgbr6510s203:30.126L24   RAID5   DGC     217.3 GB
Block     6006016083402B004DE576D7
    6   vgbr6510s203:30.126L25   RAID5   DGC     423.5 GB  local
Block     6006016083402B003CF93694
    7   vgci9710s202:2-24.0L26   RAID5   DGC     423.5 GB
Block     6006016083402B003DF93694
```

3. Select the index number corresponding to the array LUN you want to assign as the root volume.

   The array LUN must be of sufficient size to create the root volume.

   The array LUN selected for root volume creation is marked "local (root)".

   In the following example, the array LUN with index number 3 is marked for root volume creation:

```
The root volume will be created on switch 0:5.183L33.

**ONTAP requires that 11.0 GB of space be reserved for use in diagnostic
and recovery
operations.**  Select one array LUN to be used as spare for diagnostic
and recovery operations.

Index Array LUN Name    Model       Vendor    Size   Owner
Checksum  Serial Number
----- ---------------- ----------  ------  -------- -------------
--------  ------------------------
   0  switch0:5.183L1   SYMMETRIX   EMC     266.1 GB
Block     600604803436313734316631
   1  switch0:5.183L3   SYMMETRIX   EMC     266.1 GB
Block     600604803436316333353837
   2  switch0:5.183L31  SYMMETRIX   EMC     266.1 GB
Block     600604803436313237643666
   3  switch0:5.183L33  SYMMETRIX   EMC     658.3 GB local  (root)
Block     600604803436316263613066
   4  switch0:7.183L0   SYMMETRIX   EMC     173.6 GB
Block     600604803436313261356235
   5  switch0:7.183L2   SYMMETRIX   EMC     173.6 GB
Block     600604803436313438396431
   6  switch0:7.183L4   SYMMETRIX   EMC     658.3 GB
Block     600604803436313161663031
   7  switch0:7.183L30  SYMMETRIX   EMC     173.6 GB
Block     600604803436316538353834
   8  switch0:7.183L32  SYMMETRIX   EMC     266.1 GB
Block     600604803436313237353738
   9  switch0:7.183L34  SYMMETRIX   EMC     658.3 GB
Block     600604803436313737333662
```

4. Select the index number corresponding to the array LUN you want to assign for use in diagnostic and recovery options.

   The array LUN must be of sufficient size for use in diagnostic and recovery options. If required, you can also select multiple array LUNs with a combined size greater than or equal to the specified size. To select multiple entries, you must enter the comma-separated values of all of the index numbers corresponding to the array LUNs you want to select for diagnostic and recovery options.

   The following example shows a list of array LUNs selected for root volume creation and for diagnostic and recovery options:

```
Here is a list of the selected array LUNs
Index Array LUN Name     Model      Vendor    Size     Owner
Checksum  Serial Number
----- -----------------  ---------  ------  --------  -------------
--------  ------------------------
   2  switch0:5.183L31   SYMMETRIX  EMC     266.1 GB  local
Block     600604803436313237643666
   3  switch0:5.183L33   SYMMETRIX  EMC     658.3 GB  local    (root)
Block     600604803436316263613066
   4  switch0:7.183L0    SYMMETRIX  EMC     173.6 GB  local
Block     600604803436313261356235
   5  switch0:7.183L2    SYMMETRIX  EMC     173.6 GB  local
Block     600604803436313438396431
Do you want to continue (yes|no)?
```

> Selecting “no” clears the LUN selection.

5. Enter **`y`** when prompted by the system to continue with the installation process.

   The root aggregate and the root volume are created and the rest of the installation process continues.

6. Enter the required details to create the node management interface.

   The following example shows the node management interface screen with a message confirming the creation of the node management interface:

```
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.

Enter the node management interface port [e0M]:
Enter the node management interface IP address: 192.0.2.66

Enter the node management interface netmask: 255.255.255.192
Enter the node management interface default gateway: 192.0.2.7
A node management interface on port e0M with IP address 192.0.2.66 has
been created.

This node has its management address assigned and is ready for cluster
setup.
```

After you finish

After configuring ONTAP on all of the nodes that you want to use with array LUNs, you should complete the Cluster setup process

Related information

FlexArray virtualization installation requirements and reference

Setting up the cluster

Setting up the cluster involves setting up each node, creating the cluster on the first node, and joining any remaining nodes to the cluster.

Related information

Software setup

Installing the license for using array LUNs in a MetroCluster configuration

You must install the V_StorageAttach license on each MetroCluster node that you want to use with array LUNs. You cannot use array LUNs in an aggregate until the license is installed.

Before you begin

- The cluster must be installed.
- You must have the license key for the V_StorageAttach license.

About this task

You must use a separate license key for each node on which you want to install the V_StorageAttach license.

Steps

1. Install the V_StorageAttach license.

   `system license add`

   Repeat this step for each cluster node on which you want to install the license.

2. Verify that the V_StorageAttach license is installed on all required nodes in a cluster.

   `system license show`

   The following sample output shows that the V_StorageAttach license is installed on the nodes of cluster_A:

```
cluster_A::> system license show
Serial Number: nnnnnnnn
Owner: controller_A_1
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
V_StorageAttach   license Virtual Attached Storage


Serial Number: llllllll
Owner: controller_A_2
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
V_StorageAttach   license Virtual Attached Storage
```

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.

> Converting an FC port to an FC-VI port with the `ucadmin` command is only supported on the FAS8020 and AFF 8020 systems. Converting FC ports to FCVI ports is not supported on any other platform.

Steps

1. Disable the ports:

   `storage disable adapter 1a`

`storage disable adapter 1b`

```
*> 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`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

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).

```
*> 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`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Shut down the controller, and then reboot into Maintenance mode.
6. Confirm the configuration change:

   `ucadmin show local`

```
Node            Adapter  Mode     Type       Mode     Type       Status
------------    -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
                1a       fc       fcvi       -        -          online
controller_B_1
                1b       fc       fcvi       -        -          online
controller_B_1
                1c       fc       initiator  -        -          online
controller_B_1
                1d       fc       initiator  -        -          online
6 entries were displayed.
```

Assigning ownership of array LUNs

Array LUNs must be owned by a node before they can be added to an aggregate to be used as storage.

Before you begin

- Back-end configuration testing (testing of the connectivity and configuration of devices behind the ONTAP systems) must be completed.
- Array LUNs that you want to assign must be presented to the ONTAP systems.

About this task

You can assign ownership of array LUNs that have the following characteristics:

- They are unowned.
- They have no storage array configuration errors, such as the following:
  - The array LUN is smaller than or larger than the size that ONTAP supports.
  - The LDEV is mapped on only one port.
  - The LDEV has inconsistent LUN IDs assigned to it.
  - The LUN is available on only one path.

ONTAP issues an error message if you try to assign ownership of an array LUN with back-end configuration errors that would interfere with the ONTAP system and the storage array operating together. You must fix such errors before you can proceed with array LUN assignment.

ONTAP alerts you if you try to assign an array LUN with a redundancy error: for example, all paths to this array LUN are connected to the same controller or only one path to the array LUN. You can fix a redundancy error before or after assigning ownership of the LUN.

Steps

1. View the array LUNs that have not yet been assigned to a node:

   ```
   storage disk show -container-type unassigned
   ```

2. Assign an array LUN to this node:

   `storage disk assign -disk` *`array_LUN_name`* `-owner` *`nodename`*

   If you want to fix a redundancy error after disk assignment instead of before, you must use the `-force` parameter with the storage disk assign command.

Related information

FlexArray virtualization installation requirements and reference

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. Configure intercluster LIFs using the procedure in:

   Configuring intercluster LIFs

2. Create a cluster peer relationship using the procedure in:

   Peering the clusters

Mirroring the root aggregates

You must mirror the root aggregates in your MetroCluster configuration to ensure data protection.

Before you begin

You must have ensured that the SyncMirror requirements for the MetroCluster configuration with array LUNs are satisfied. Refer to Requirements for a MetroCluster configuration with array LUNs.

About this task

You must repeat this task for each controller in the MetroCluster configuration.

Step

1. Mirror the unmirrored root aggregate:

   `storage aggregate mirror`

   The following command mirrors the root aggregate for controller_A_1:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   The root aggregate is mirrored with array LUNs from pool1.

Creating data aggregates on, implementing, and verifying the MetroCluster configuration

You must create data aggregates on each node, implement, and verify the MetroCluster configuration.

Steps

1. Create data aggregates on each node:
   a. Create a mirrored data aggregate on each node:

      Mirror the root aggregates.

   b. If needed, create unmirrored data aggregates:

      Create a mirrored data aggregate on each node.

2. Implement the MetroCluster configuration.
3. Configure the MetroCluster FC switches for health monitoring.
4. Check and verify the configuration:
   a. Check the MetroCluster configuration.
   b. Check for MetroCluster configuration errors with Config Advisor.
   c. Verify switchover, healing, and switchback.
5. Install and configure the MetroCluster Tiebreaker software:
   a. Install the Tiebreaker Software.
   b. Configure the Tiebreaker Software.
6. Set the destination for configuration backup files:

   Protect configuration backup files.

Implementing a MetroCluster configuration with both disks and array LUNs

To implement a MetroCluster configuration with native disks and array LUNs, you must ensure that the ONTAP systems used in the configuration can attach to storage arrays.

A MetroCluster configuration with disks and array LUNs can have either two or four nodes. Although the four-node MetroCluster configuration must be fabric-attached, the two-node configuration can either be stretch or fabric-attached.

In the NetApp Interoperability Matrix Tool (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.

Related information

For setting up a two-node fabric-attached MetroCluster configuration or a four-node MetroCluster configuration with native disks and array LUNs, you must use FC-to-SAS bridges to connect the ONTAP systems with the disk shelves through the FC switches. You can connect array LUNs through the FC switches to the ONTAP systems.

Example of a two-node fabric-attached MetroCluster configuration with disks and array LUNs

Example of a four-node MetroCluster configuration with disks and array LUNs

Considerations when implementing a MetroCluster configuration with disks and array LUNs

When planning your MetroCluster configuration for use with disks and array LUNs, you must consider various factors, such as the order of setting up access to storage, root aggregate location, and the usage of FC initiator ports, switches, and FC-to-SAS bridges.

Consider the information in the following table when planning your configuration:

Consideration	Guideline
Order of setting up access to the storage	You can set up access to either disks or array LUNs first. You must complete all setup for that type of storage and verify that it is set up correctly before setting up the other type of storage.
Location of the root aggregate	• If you are setting up a *new* MetroCluster deployment with both disks and array LUNs, you must create the root aggregate on native disks. When doing this, ensure that *at least one* disk shelf (with 24 disk drives) is set up at each of the sites. • If you are adding native disks to an *existing* MetroCluster configuration that uses array LUNs, the root aggregate can remain on an array LUN.

Using switches and FC-to-SAS bridges	FC-to-SAS bridges are required in four-node configurations and two-node fabric-attached configurations to connect the ONTAP systems to the disk shelves through the switches. You must use the same switches to connect to the storage arrays and the FC-to-SAS bridges.
Using FC initiator ports	The initiator ports used to connect to an FC-to-SAS bridge must be different from the ports used to connect to the switches, which connect to the storage arrays. A minimum of eight initiator ports is required to connect an ONTAP system to both disks and array LUNs.

Related information

- Switch configuration procedures and commands are different, depending on the switch vendor.

  Configuring the Brocade FC switches manually

  Configuring the Cisco FC switches manually

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

  Installing FC-to-SAS bridges and SAS disk shelves

- Switch zoning defines paths between connected nodes. Configuring the zoning enables you to define which array LUNs can be viewed by a specific ONTAP system.

  Example of switch zoning in a four-node MetroCluster configuration with array LUNs

  Example of switch zoning in an eight-node MetroCluster configuration with array LUNs

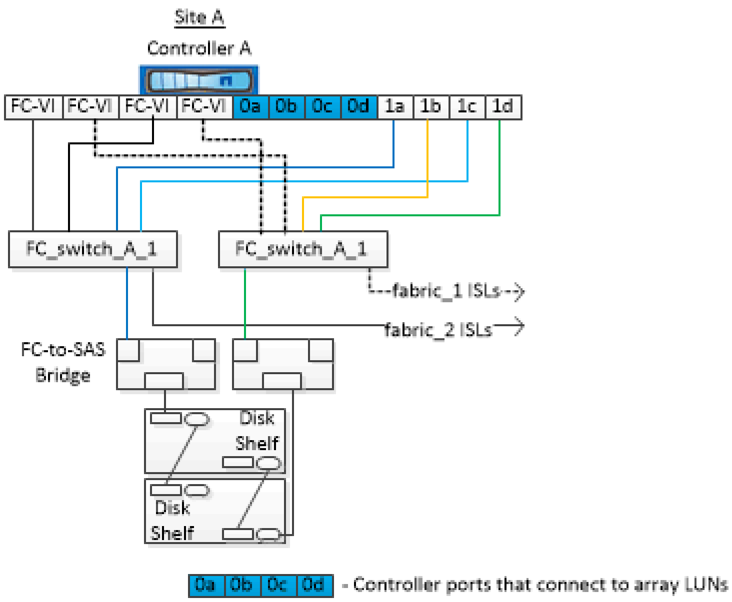
- NetApp Hardware Universe

Example of a two-node fabric-attached MetroCluster configuration with disks and array LUNs

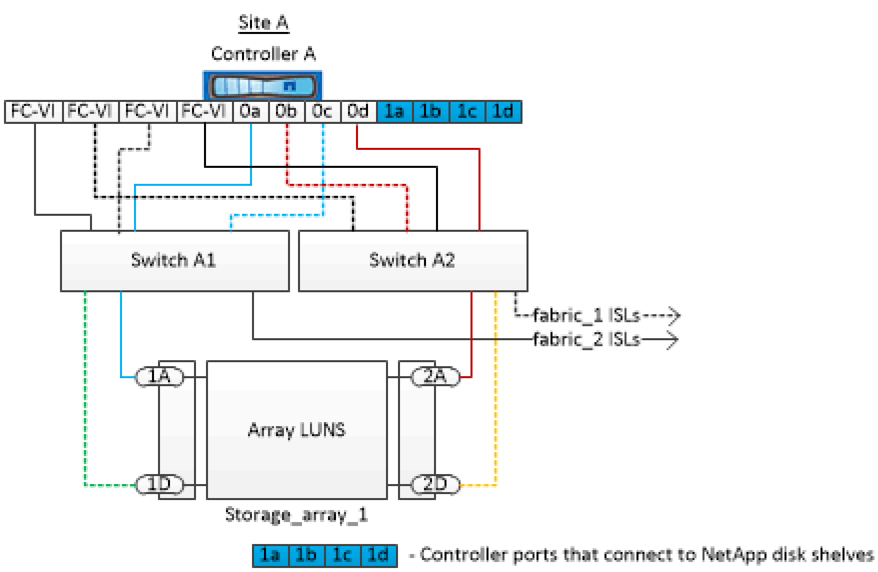
For setting up a two-node fabric-attached MetroCluster configuration with native disks and array LUNs, you must use FC-to-SAS bridges to connect the ONTAP systems with the disk shelves through the FC switches. You can connect array LUNs through the FC switches to the ONTAP systems.

The following illustrations represent examples of a two-node fabric-attached MetroCluster configuration with disks and array LUNs. They both represent the same MetroCluster configuration; the representations for disks and array LUNs are separated only for simplification.

In the following illustration showing the connectivity between ONTAP systems and disks, the HBA ports 1a through 1d are used for connectivity with disks through the FC-to-SAS bridges:



In the following illustration showing the connectivity between ONTAP systems and array LUNs, the HBA ports 0a through 0d are used for connectivity with array LUNs because ports 1a through 1d are used for connectivity with disks:



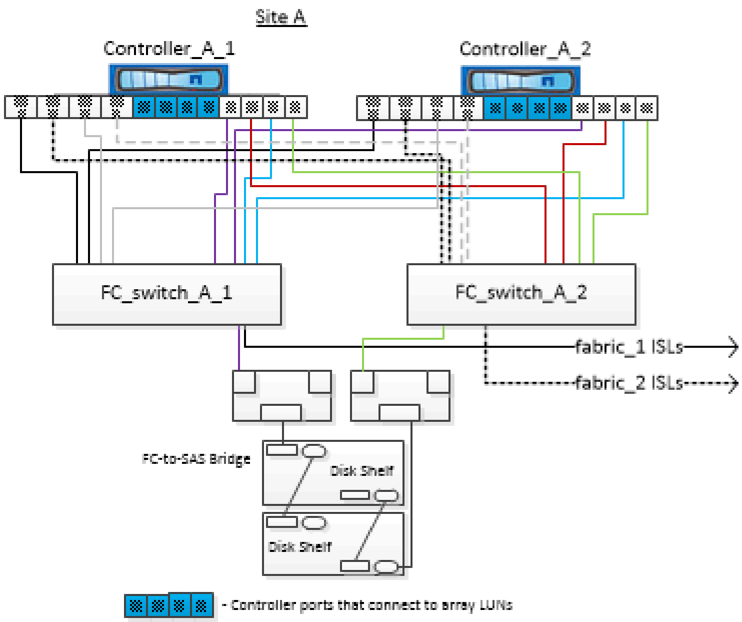
Example of a four-node MetroCluster configuration with disks and array LUNs

For setting up a four-node MetroCluster configuration with native disks and array LUNs, you must use FC-to-SAS bridges to connect the ONTAP systems with the disk shelves through the FC switches. You can connect array LUNs through the FC switches to the ONTAP systems.

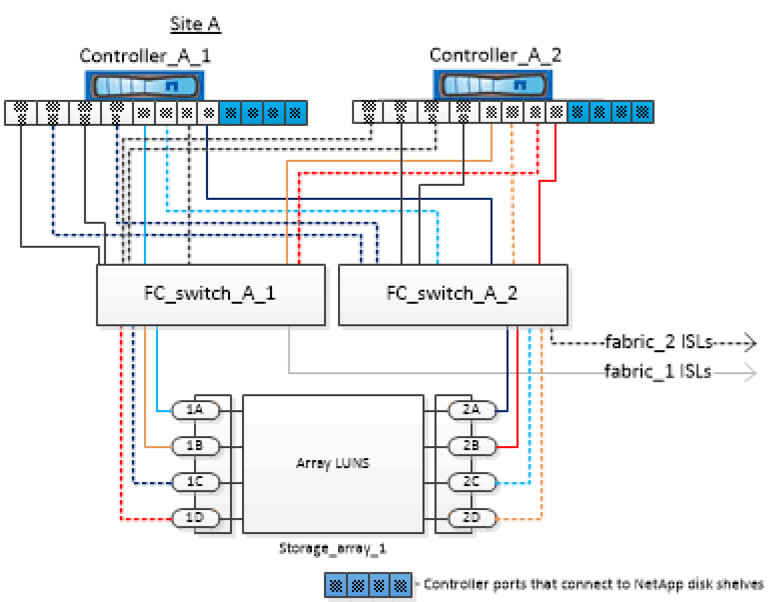
A minimum of eight initiator ports is required for an ONTAP system to connect to both native disks and array LUNs.

The following illustrations represent examples of a MetroCluster configuration with disks and array LUNs. They both represent the same MetroCluster configuration; the representations for disks and array LUNs are separated only for simplification.

In the following illustration that shows the connectivity between ONTAP systems and disks, the HBA ports 1a through 1d are used for connectivity with disks through the FC-to-SAS bridges:



In the following illustration that shows the connectivity between ONTAP systems and array LUNs, the HBA ports 0a through 0d are used for connectivity with array LUNs because ports 1a through 1d are used for connectivity with disks:



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, FC switches, and 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.

MetroCluster operations in ONTAP System Manager

Depending on your ONTAP version, some MetroCluster-specific operations can be performed using ONTAP System Manager.

- Switchover and switchback in MetroCluster IP configurations (starting in ONTAP 9.7).
- Provision and grow of mirrored aggregates in the MetroCluster IP configurations (starting in ONTAP 9.8).

  Unmirrored aggregates are not supported in System Manager.

FlexCache support in a MetroCluster configuration

Starting with ONTAP 9.7, FlexCache volumes are supported on MetroCluster configurations. You should be aware of requirements for manual repeering after switchover or switchback operations.

SVM repeering after switchover when FlexCache origin and cache are within the same MetroCluster site

After a negotiated or unplanned switchover, any SVM FlexCache peering relationship within the cluster must be manually configured.

For example, SVMs "vs1" (cache) and "vs2" (origin) are on site_A. These SVMs are peered.

After switchover, SVMs "vs1-mc" and "vs2-mc" are activated at the partner site (site_B). They must be manually repeered for FlexCache to work using the `vserver peer repeer` command.

SVM repeering after switchover or switchback when a FlexCache destination is on a third cluster and in disconnected mode

For FlexCache relationships to a cluster outside of the MetroCluster configuration, the peering must always be manually reconfigured after a switchover if the involved clusters are in disconnected mode during switchover.

For example:

- One end of the FlexCache (cache_1 on vs1) resides on MetroCluster site_A.
- The other end of the FlexCache (origin_1 on vs2) resides on site_C (not in the MetroCluster configuration).

When switchover is triggered, and if site_A and site_C are not connected, you must manually repeer the SVMs on site_B (the switchover cluster) and site_C using the `vserver peer repeer` command after the switchover.

When switchback is performed, you must again repeer the SVMs on site_A (the original cluster) and site_C.

Related information

FlexCache volumes management

FabricPool support in MetroCluster configurations

Starting with ONTAP 9.7, MetroCluster configurations support FabricPool storage tiers.

For general information on using FabricPools, see the Disks and Aggregates Power Guide

Considerations when using FabricPools

- The clusters must have FabricPool licenses with matching capacity limits.
- The clusters must have IPspaces with matching names.

  This can be the default IPspace, or an IPspace that an administer has created. This IPspace will be used for FabricPool object store configuration setups.

- For the selected IPspace, each cluster must have an intercluster LIF defined that can reach the external object store

Configuring an aggregate for use in a mirrored FabricPool

> Before you configure the aggregate, you must set up object stores as described in "Setting up object stores for FabricPool in a MetroCluster configuration" in the Disks and Aggregates Power Guide

Steps

To configure an aggregate for use in a FabricPool:

1. Create the aggregate or select an existing aggregate.
2. Mirror the aggregate as a typical mirrored aggregate within the MetroCluster configuration.
3. Create the FabricPool mirror with the aggregate, as described in the Disks and Aggregates Power Guide
   a. Attach a primary object store.

      This object store is physically closer to the cluster.

   b. Add a mirror object store.

      This object store is physically further distant to the cluster than the primary object store.

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).

> 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

- Network and LIF management
- 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 object replication and subnet configuration requirements

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

  Requirements for LIF creation in a MetroCluster configuration

- 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.

  LIF replication and placement requirements and issues

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                     Broadcast                   Avail/
Name      Subnet           Domain    Gateway           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                     Broadcast                   Avail/
Name      Subnet           Domain    Gateway           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.

Related information

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

  Requirements for LIF creation in a MetroCluster configuration

- 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.

  LIF replication and placement requirements and issues

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
- NFS and SAN configurations: You must use different storage virtual machines (SVMs) for both the unmirrored and mirrored aggregates

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.

Related information

- 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 object replication and subnet configuration requirements

- 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.

  LIF replication and placement requirements and 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:

Condition	LIF type: FC	LIF type: IP/iSCSI

Node identification	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.	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.
Port identification	ONTAP identifies the connected FC target ports on the DR cluster.	The ports on the DR cluster that are in the same IPspace as the source LIF are selected for a reachability check. If there are no ports in the DR cluster in the same IPspace, the LIF cannot be placed. All of the ports in the DR cluster that are already hosting a LIF in the same IPspace and subnet are automatically marked as reachable; and can be used for placement. These ports are not included in the reachability check.
Reachability check	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.	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.

Port selection	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.	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.
LIF placement	From the reachable ports, ONTAP selects the least loaded port for placement.	From the selected ports, ONTAP selects the least loaded port for placement.

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.

> 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.

LIFs inaccessible after a switchover

If any change is made in the FC switch fabric to which the FC target ports of the source and DR nodes are connected, then the FC LIFs that are placed at the DR partner might become inaccessible to the hosts after a switchover operation.

You should run the `metrocluster check lif repair-placement` command on the source as well as the DR nodes after a change is made in the FC switch fabric to verify the host connectivity of LIFs. The changes in the switch fabric might result in LIFs getting placed in different target FC ports at the DR partner node.

Related information

- 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 object replication and subnet configuration requirements

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

  Requirements for LIF creation in a MetroCluster configuration

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.

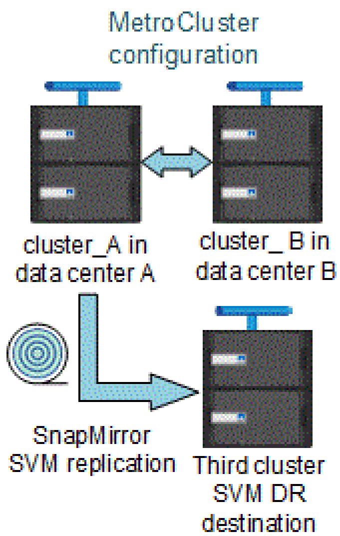
You should be aware of the following requirements and limitations of using SVMs with SnapMirror disaster recovery:

- 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.

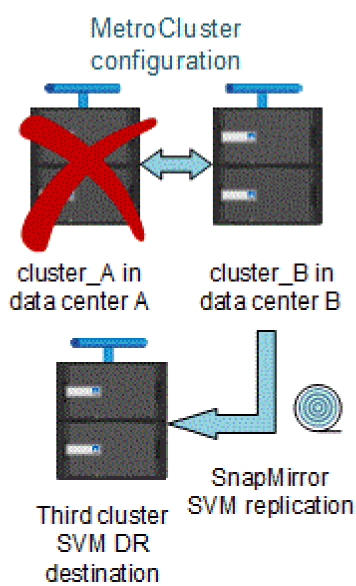
- When a MetroCluster configuration is in a steady state, the MetroCluster sync-destination SVM cannot be the source of an SVM disaster recovery relationship, since the volumes are not online.

  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:



- During the switchover and switchback processes, replication to the SVM DR destination might fail.

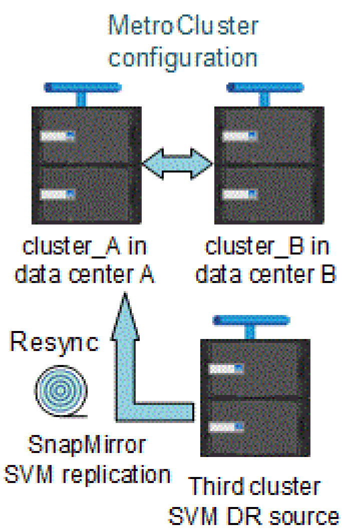
  However, after the switchover or switchback process completes, the next SVM DR scheduled updates will succeed.

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

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 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

> 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`**

Where to find additional information

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

MetroCluster and miscellaneous guides

Guide	Content
ONTAP 9 Documentation Center	• All MetroCluster guides
NetApp MetroCluster Solution Architecture and Design, TR-4705	• A technical overview of the MetroCluster FC configuration and operation. • Best practices for MetroCluster FC configuration.
MetroCluster IP Solution Architecture and Design, TR-4689	• A technical overview of the MetroCluster IP configuration and operation. • Best practices for MetroCluster IP configuration.
Stretch MetroCluster installation and configuration	• Stretch MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • 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
MetroCluster Maintenance Guide	• Guidelines for maintenance in a MetroCluster FC configuration • Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches • Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster FC configuration • Expanding a two-node fabric-attached or stretch MetroCluster FC configuration to a four-node MetroCluster configuration. • Expanding a four-node fabric-attached or stretch MetroCluster FC configuration to an eight-node MetroCluster FC configuration.
MetroCluster Transition Guide MetroCluster Upgrade and Expansion Guide	• Upgrading or refreshing a MetroCluster configuration • Transitioning from a MetroCluster FC configuration to a MetroCluster IP configuration • Expanding a MetroCluster configuration by adding additional nodes
MetroCluster Tiebreaker Software Installation and Configuration Guide	• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software
Active IQ Digital Advisor documentation NetApp Documentation: Product Guides and Resources	• Monitoring the MetroCluster configuration and performance
Copy-based transition	• Transitioning data from 7-Mode storage systems to clustered storage systems
ONTAP concepts	• How mirrored aggregates work

MetroCluster IP Installation and Configuration Guide

This guide describes how to install and configure the MetroCluster IP hardware and software components.

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

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

General information about ONTAP and MetroCluster configurations is also available.

ONTAP 9 Documentation Center

Preparing for the MetroCluster IP installation

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

Differences among the ONTAP MetroCluster configurations

Differences between ONTAP MetroCluster configurations

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

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

Feature	IP configurations	Fabric attached configurations		Stretch configurations	
		Four- or eight-node	**Two-node**	**Two-node bridge-attached**	**Two-node direct-attached**
Number of controllers	Four or eight*	Four or eight	Two	Two	Two
Uses an FC switch storage fabric	No	Yes	Yes	No	No
Uses an IP switch storage fabric	Yes	No	No	No	No

Uses FC-to-SAS bridges	No	Yes	Yes	Yes	No
Uses direct-attached SAS storage	Yes (local attached only)	No	No	No	Yes
Supports ADP	Yes (starting in ONTAP 9.4)	No	No	No	No
Supports local HA	Yes	Yes	No	No	No
Supports ONTAP AUSO	No	Yes	Yes	Yes	Yes
Supports unmirrored aggregates	Yes (starting in ONTAP 9.8)	Yes	Yes	Yes	Yes
Supports array LUNs	No	Yes	Yes	Yes	Yes
Supports ONTAP Mediator	Yes (starting in ONTAP 9.7)	No	No	No	No
Supports MetroCluster Tiebreaker	Yes (not in combination with ONTAP Mediator)	Yes	Yes	Yes	Yes
Supports All SAN Arrays	Yes	Yes	Yes	Yes	Yes

Important

Notice the following considerations for eight-node MetroCluster IP configurations:

- Eight-node configurations are supported starting in ONTAP 9.9.1.
- Only NetApp-validated MetroCluster switches (ordered from NetApp) are supported.
- Configurations using IP-routed (layer 3) backend connections are not supported.
- Configurations using shared private layer 2 networks are not supported.
- Configurations using a Cisco 9336C-FX2 shared switch are not supported.

Support for All SAN Array systems in MetroCluster configurations

Some of the All SAN Arrays (ASAs) are supported in MetroCluster configurations. In the MetroCluster documentation, the information for AFF models applies to the corresponding ASA system. For example, all cabling and other information for the AFF A400 system also applies to the ASA AFF A400 system.

Supported platform configurations are listed in the NetApp Hardware Universe.

Differences between ONTAP Mediator and MetroCluster Tiebreaker

Starting with ONTAP 9.7, you can use either the ONTAP Mediator-assisted automatic unplanned switchover (MAUSO) in the MetroCluster IP configuration or you can use the MetroCluster Tiebreaker software. Only one of the two services can be used with the MetroCluster IP configuration.

The different MetroCluster configurations perform automatic switchover under different circumstances:

- **MetroCluster FC configurations using the AUSO capability (not present in MetroCluster IP configurations)**

  In these configurations, AUSO is initiated if controllers fail but the storage (and bridges, if present) remain operational.

- **MetroCluster IP configurations using the ONTAP Mediator service (ONTAP 9.7 and later)**

  In these configurations, MAUSO is initiated in the same circumstances as AUSO, as described above, and also after a complete site failure (controllers, storage, and switches).

  > MAUSO is initiated only if nonvolatile cache mirroring (*DR mirroring*) and SyncMirror plex mirroring is in sync at the time of the failure.

- **MetroCluster IP or FC configurations using the Tiebreaker software in active mode**

  In these configurations, the Tiebreaker initiates unplanned switchover after a complete site failure.

  Before using the Tiebreaker software, review the MetroCluster Tiebreaker Software Installation and Configuration Guide

Interoperability of ONTAP Mediator with other applications and appliances

You cannot use any third-party applications or appliances that can trigger a switchover in combination with ONTAP Mediator. In addition, monitoring a MetroCluster configuration with MetroCluster Tiebreaker software is not supported when using ONTAP Mediator.

How the ONTAP Mediator supports automatic unplanned switchover

The ONTAP Mediator stores state information about the MetroCluster nodes in mailboxes located on the Mediator host. The MetroCluster nodes can use this information to monitor the state of their DR partners and implement a Mediator-assisted automatic unplanned switchover (MAUSO) in the case of a disaster.

When a node detects a site failure requiring a switchover, it takes steps to confirm that the switchover is appropriate and, if so, performs the switchover.

MAUSO is only initiated if both SyncMirror mirroring and DR mirroring of each node’s nonvolatile cache is operating and the caches and mirrors are synchronized at the time of the failure.

Considerations for MetroCluster IP configurations

You should understand how the controllers access the remote storage and how the MetroCluster IP addresses work.

Access to remote storage in MetroCluster IP configurations

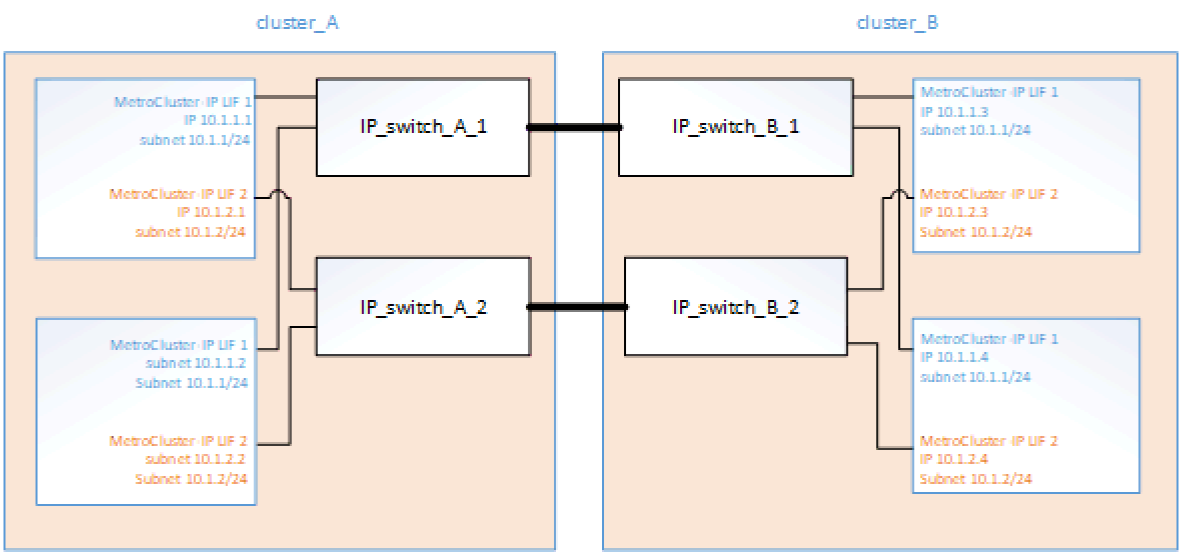
In MetroCluster IP configurations, the only way the local controllers can reach the remote storage pools is via the remote controllers. The IP switches are connected to the Ethernet ports on the controllers; they do not have direct connections to the disk shelves. If the remote controller is down, the local controllers cannot reach their remote storage pools.

This is different than MetroCluster FC configurations, in which the remote storage pools are connected to the local controllers via the FC fabric or the SAS connections. The local controllers still have access to the remote storage even if the remote controllers are down.

MetroCluster IP addresses

You should be aware of how the MetroCluster IP addresses and interfaces are implemented in a MetroCluster IP configuration, as well as the associated requirements.

In a MetroCluster IP configuration, replication of storage and nonvolatile cache between the HA pairs and the DR partners is performed over high-bandwidth dedicated links in the MetroCluster IP fabric. iSCSI connections are used for storage replication. The IP switches are also used for all intra-cluster traffic within the local clusters. The MetroCluster traffic is kept separate from the intra-cluster traffic by using separate IP subnets and VLANs. The MetroCluster IP fabric is distinct and different from the cluster peering network.



The MetroCluster IP configuration requires two IP addresses on each node that are reserved for the back-end MetroCluster IP fabric. The reserved IP addresses are assigned to MetroCluster IP logical interfaces (LIFs) during initial configuration, and have the following requirements:

> You must choose the MetroCluster IP addresses carefully because you cannot change them after initial configuration.

- They must fall in a unique IP range.

  They must not overlap with any IP space in the environment.

* They must reside in one of two IP subnets that separate them from all other traffic.

For example, the nodes might be configured with the following IP addresses:

Node	Interface	IP address	Subnet
node_A_1	MetroCluster IP interface 1	10.1.1.1	10.1.1/24
node_A_1	MetroCluster IP interface 2	10.1.2.1	10.1.2/24
node_A_2	MetroCluster IP interface 1	10.1.1.2	10.1.1/24
node_A_2	MetroCluster IP interface 2	10.1.2.2	10.1.2/24
node_B_1	MetroCluster IP interface 1	10.1.1.3	10.1.1/24
node_B_1	MetroCluster IP interface 2	10.1.2.3	10.1.2/24
node_B_2	MetroCluster IP interface 1	10.1.1.4	10.1.1/24
node_B_2	MetroCluster IP interface 2	10.1.2.4	10.1.2/24

Characteristics of MetroCluster IP interfaces

The MetroCluster IP interfaces are specific to MetroCluster IP configurations. They have different characteristics from other ONTAP interface types:

* They are created by the `metrocluster configuration-settings interface create` command as part the initial MetroCluster configuration.

  > Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.

  They are not created or modified by the network interface commands.

* They do not appear in the output of the `network interface show` command.
* They do not fail over, but remain associated with the port on which they were created.
* MetroCluster IP configurations use specific Ethernet ports (depending on the platform) for the MetroCluster IP interfaces.

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Starting with ONTAP 9.4, MetroCluster IP configurations support new installations with AFF systems using ADP (Advanced Drive Partitioning). In most configurations, partitioning and disk assignment are performed automatically during the initial configuration of the MetroCluster sites.

ONTAP 9.4 and later releases include the following changes for ADP support:

- Pool 0 disk assignments are done at the factory.
- The unmirrored root is created at the factory.
- Data partition assignment is done at the customer site during the setup procedure.
- In most cases, drive assignment and partitioning is done automatically during the setup procedures.

> When upgrading from ONTAP 9.4 to 9.5, the system recognizes the existing disk assignments.

Automatic partitioning

ADP is performed automatically during initial configuration of the platform.

> Starting with ONTAP 9.5, `disk auto=assignment` must be enabled for automatic partitioning for ADP to occur.

How shelf-by-shelf automatic assignment works

If there are four external shelves per site, each shelf is assigned to a different node and different pool, as shown in the following example:

- All of the disks on site_A-shelf_1 are automatically assigned to pool 0 of node_A_1
- All of the disks on site_A-shelf_3 are automatically assigned to pool 0 of node_A_2
- All of the disks on site_B-shelf_1 are automatically assigned to pool 0 of node_B_1
- All of the disks on site_B-shelf_3 are automatically assigned to pool 0 of node_B_2
- All of the disks on site_B-shelf_2 are automatically assigned to pool 1 of node_A_1
- All of the disks on site_B-shelf_4 are automatically assigned to pool 1 of node_A_2
- All of the disks on site_A-shelf_2 are automatically assigned to pool 1 of node_B_1
- All of the disks on site_A-shelf_4 are automatically assigned to pool 1 of node_B_2

How to populate partially-full shelves

If your configuration is using shelves that are not fully populated (have empty drive bays) you must distribute the drives evenly throughout the shelf, depending on the disk assignment policy. The disk assignment policy depends on how many shelves are at each MetroCluster site.

If you are using a single shelf at each site (or just the internal shelf on an AFF A800 system), disks are assigned using a quarter-shelf policy. If the shelf is not fully populated, install the drives equally on all quarters.

The following table shows an example of how to place 24 disks in a 48 drive internal shelf. The ownership for the drives is also shown.

The 48 drive bays are divided into four quarters:	Install six drives in the first six bays in each quarter…
Quarter 1: Bays 0 -11	Bays 0-5
Quarter 2: Bays 12-23	Bays 12-17
Quarter 3: Bays 24-35	Bays 24-29
Quarter 4: Bays 36-48	Bays 36-41

If you are using two shelves at each site, disks are assigned using a half-shelf policy. If the shelves are not fully populated, install the drives equally from either end of the shelf.

For example, if you are installing 12 drives in a 24 drive shelf, install drives in bays 0-5 and 18-23.

Manual drive assignment (ONTAP 9.5)

In ONTAP 9.5, manual drive assignment is required on systems with the following shelf configurations:

- Three external shelves per site.

  Two shelves are assigned automatically using a half-shelf assignment policy, but the third shelf must be assigned manually.

- More than four shelves per site and the total number of external shelves is not a multiple of four.

  Extra shelves above the nearest multiple of four are left unassigned and the drives must be assigned manually. For example, if there are five external shelves at the site, shelf five must be assigned manually.

You only need to manually assign a single drive on each unassigned shelf. The rest of the drives on the shelf are then automatically assigned.

Manual drive assignment (ONTAP 9.4)

In ONTAP 9.4, manual drive assignment is required on systems with the following shelf configurations:

- Fewer than four external shelves per site.

  The drives must be assigned manually to ensure symmetrical assignment of the drives, with each pool having an equal number of drives.

- More than four external shelves per site and the total number of external shelves is not a multiple of four.

  Extra shelves above the nearest multiple of four are left unassigned and the drives must be assigned manually.

When manually assigning drives, you should assign disks symmetrically, with an equal number of drives assigned to each pool. For example, if the configuration has two storage shelves at each site, you would one shelf to the local HA pair and one shelf to the remote HA pair:

- Assign half of the disks on site_A-shelf_1 to pool 0 of node_A_1.
- Assign half of the disks on site_A-shelf_1 to pool 0 of node_A_2.
- Assign half of the disks on site_A-shelf_2 to pool 1 of node_B_1.
- Assign half of the disks on site_A-shelf_2 to pool 1 of node_B_2.
- Assign half of the disks on site_B-shelf_1 to pool 0 of node_B_1.
- Assign half of the disks on site_B-shelf_1 to pool 0 of node_B_2.
- Assign half of the disks on site_B-shelf_2 to pool 1 of node_A_1.
- Assign half of the disks on site_B-shelf_2 to pool 1 of node_A_2.

Adding shelves to an existing configuration.

Automatic drive assignment supports the symmetrical addition of shelves to an existing configuration.

When new shelves are added, the system applies the same assignment policy to newly added shelves. For example, with a single shelf per site, if an additional shelf is added, the systems applies the quarter-shelf assignment rules to the new shelf.

Related information

Required MetroCluster IP components and naming conventions

Disk and aggregate management

ADP and disk assignment differences by system in MetroCluster IP configurations

The operation of Advanced Drive Partitioning (ADP) and automatic disk assignment in MetroCluster IP configurations varies depending on the system model.

> In systems using ADP, aggregates are created using partitions in which each drive is partitioned in to P1, P2 and P3 partitions. The root aggregate is created using P3 partitions.

You must meet the MetroCluster limits for the maximum number of supported drives and other guidelines.

NetApp Hardware Universe

ADP and disk assignment on AFF A320 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition

Minimum recommended shelves (per site)	Two shelves	The drives on each external shelf are divided into two equal groups (halves). Each half-shelf is automatically assigned to a separate pool.	One shelf is used by the local HA pair. The second shelf is used by the remote HA pair. **Partitions on each shelf are used to create the root aggregate. Each of the two plexes in the root aggregate includes the following partitions** • Eight partitions for data • Two parity partitions • Two spare partitions
Minimum supported shelves (per site)	One shelf	The drives are divided into four equal groups. Each quarter-shelf is automatically assigned to a separate pool.	Each of the two plexes in the root aggregate includes the following partitions: • Three partitions for data • Two parity partitions • One spare partition

ADP and disk assignment on AFF A220 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition

Minimum recommended shelves (per site)	Internal drives only	The internal drives are divided into four equal groups. Each group is automatically assigned to a separate pool and each pool is assigned to a separate controller in the configuration. Half of the internal drives remain unassigned before MetroCluster is configured.	Two quarters are used by the local HA pair. The other two quarters are used by the remote HA pair. The root aggregate includes the following partitions in each plex: • Three partitions for data • Two parity partitions • One spare partition

Minimum supported shelves (per site)	16 internal drives	The drives are divided into four equal groups. Each quarter-shelf is automatically assigned to a separate pool. Two quarters on a shelf can have the same pool. The pool is chosen based on the node that owns the quarter: • If owned by the local node, pool0 is used. • If owned by the remote node, pool1 is used. For example: a shelf with quarters Q1 through Q4 can have following assignments: • Q1: node_A_1 pool0 • Q2: node_A_2 pool0 • Q3: node_B_1 pool1 • Q4:node_B_2 pool1 Half of the internal drives remain unassigned before MetroCluster is configured.	Each of the two plexes in the root aggregate includes the following partitions: • One partition for data • Two parity partitions • One spare partition

ADP and disk assignment on AFF A250 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition

Minimum recommended shelves (per site)	Two shelves	The drives on each external shelf are divided into two equal groups (halves). Each half-shelf is automatically assigned to a separate pool.	One shelf is used by the local HA pair. The second shelf is used by the remote HA pair. Partitions on each shelf are used to create the root aggregate. The root aggregate includes the following partitions in each plex: • Eight partitions for data • Two parity partitions • Two spare partitions
Minimum supported shelves (per site)	24 internal drives only	The drives are divided into four equal groups. Each quarter-shelf is automatically assigned to a separate pool.	Each of the two plexes in the root aggregate includes the following partitions: • Three partitions for data • Two parity partitions • One spare partition

ADP and disk assignment on AFF A300 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition
Minimum recommended shelves (per site)	Two shelves	The drives on each external shelf are divided into two equal groups (halves). Each half-shelf is automatically assigned to a separate pool.	One shelf is used by the local HA pair. The second shelf is used by the remote HA pair. Partitions on each shelf are used to create the root aggregate. The root aggregate includes the following partitions in each plex: • Eight partitions for data • Two parity partitions • Two spare partitions

Minimum supported shelves (per site)	One shelf	The drives are divided into four equal groups. Each quarter-shelf is automatically assigned to a separate pool.	Each of the two plexes in the root aggregate includes the following partitions: • Three partitions for data • Two parity partitions • One spare partition

ADP and disk assignment on AFF A400 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition
Minimum recommended shelves (per site)	Four shelves	Drives are automatically assigned on a shelf-by-shelf basis.	Each of the two plexes in the root aggregate includes: • 20 partitions for data • Two parity partitions • Two spare partitions
Minimum supported shelves (per site)	One shelf	The drives are divided into four equal groups (quarters). Each quarter-shelf is automatically assigned to a separate pool.	Each of the two plexes in the root aggregate includes: • Three partitions for data • Two parity partitions • One spare partition

ADP and disk assignment on AFF A700 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition
Minimum recommended shelves (per site)	Four shelves	Drives are automatically assigned on a shelf-by-shelf basis.	Each of the two plexes in the root aggregate includes: • 20 partitions for data • Two parity partitions • Two spare partitions

Minimum supported shelves (per site)	One shelf	The drives are divided into four equal groups (quarters). Each quarter-shelf is automatically assigned to a separate pool.	Each of the two plexes in the root aggregate includes: • Three partitions for data • Two parity partitions • One spare partition

ADP and disk assignment on AFF A800 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root aggregate
Minimum recommended shelves (per site)	Internal drives and four external shelves	The internal partitions are divided into four equal groups (quarters). Each quarter is automatically assigned to a separate pool.The drives on the external shelves are automatically assigned on a shelf-by-shelf basis, with all of the drives on each shelf assigned to one of the four nodes in the MetroCluster configuration.	The root aggregate is created with 12 root partitions on the internal shelf. Each of the two plexes in the root aggregate includes: • Eight partitions for data • Two parity partitions • Two spare partitions
Minimum supported shelves (per site)	24 internal drives only	The internal partitions are divided into four equal groups (quarters). Each quarter is automatically assigned to a separate pool.	The root aggregate is created with 12 root partitions on the internal shelf. Each of the two plexes in the root aggregate includes: • Three partitions for data • Two parity partitions • One spare partitions

Disk assignment on FAS2750 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition

Minimum recommended shelves (per site)	One internal and one external shelf	The internal and external shelves are divided into two equal halves. Each half is automatically assigned to different pool	Not applicable.

Disk assignment on FAS8200 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition
Minimum supported shelves (per site)	Two shelves	The drives on the external shelves are divided into two equal groups (halves). Each half-shelf is automatically assigned to a separate pool.	Not applicable.

Disk assignment on FAS500f systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition
Minimum recommended shelves (per site)	Four shelves	Drives are automatically assigned on a shelf-by-shelf basis.	Not applicable.

Disk assignment on FAS9000 systems

Guideline	Shelves per site	Drive assignment rules	ADP layout for root partition
Minimum recommended shelves (per site)	Four shelves	Drives are automatically assigned on a shelf-by-shelf basis.	Not applicable.
Minimum supported shelves (per site)	Two shelves	The drives on the shelves are divided into two equal groups (halves). Each half-shelf is automatically assigned to a separate pool.	Minimum supported shelves (per site) (active/passive HA configuration)

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. Each MetroCluster site is configured as a peer to its partner site. You must be familiar with the prerequisites and guidelines for configuring the peering relationships. This is important when deciding on 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 connectivity between 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 used in each cluster must meet the following requirements:

- The subnet must have enough IP addresses available to allocate to one intercluster LIF per node.

  For example, in a six-node cluster, the subnet used for intercluster communication must have six available IP addresses.

Each node must have an intercluster LIF with an IP address on the intercluster network.

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

> ONTAP 9 enables you to migrate your peering networks from IPv4 to IPv6 by optionally allowing both protocols to be present simultaneously on the intercluster LIFs. In earlier releases, all intercluster relationships for an entire cluster were either IPv4 or IPv6. This meant that changing protocols was a potentially disruptive event.

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 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 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
- Bidirectional HTTPS between the intercluster LIFs

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 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. This 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 the 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. This 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 for ISLs

You should know the ISL requirements for your configuration.

Basic MetroCluster ISL requirements

The following requirements must be met for the ISLs on all MetroCluster IP configurations:

- A native-speed ISL switch port must connect to a native-speed ISL switch port.

  For example, a 40 Gbps port connects to a 40 Gbps port.

- A 10 Gbps port that is in native mode (i.e., not using a breakout cable) can connect to a 10 Gbps port that is in native mode.
- The ISLs between the MetroCluster IP switches and the customer network, as well as the ISLs between the intermediate switches, follow the same rules in terms of speed.
- The number of ISLs that are between the MetroCluster switches and the customer network switches, and the number of ISLs that are between the customer network switches, do not need to match.

  For example, the MetroCluster switches can connect using two ISLs to the intermediate switches, and the intermediate switches can connect to each other using 10 ISLs.

- The speed of ISLs that are between the MetroCluster switches and the customer network switches, and the speed of ISLs that are between the customer network switches, do not need to match.

  For example, the MetroCluster switches can connect using a 40-Gbps ISL to the intermediate switches, and the intermediate switches can connect to each other using 100-Gbps ISLs.

- The number of and speed of ISLs connecting each MetroCluster switch to the intermediate switch must be the same on both MetroCluster sites.

ISL requirements in shared layer 2 networks

When sharing ISL traffic in a shared network, you must ensure that you have adequate capacity and size the ISLs appropriately. Low latency is critical for replication of data between the MetroCluster sites. Latency issues on these connections can impact client I/O.

You should review these sections to correctly calculate the required end-to-end capacity of the ISLs. Continuous nonvolatile cache and storage replication with low latency is critical for MetroCluster configurations. The latency in the back-end network impacts the latency and throughput seen by client IO.

Latency and packet loss limits in the ISLs

The following requirements must be met for round-trip traffic between the MetroCluster IP switches at site_A and site_B, with the MetroCluster configuration in steady state operation:

- Round trip latency must be less than or equal to 7 ms.

  The maximum distance is 700 km, so the distance between the sites is limited by the latency or the maximum distance, whichever is reached first.

  As the distance between two MetroCluster sites increases, latency increases, usually in the range of 1 ms round-trip delay time per 100 km (62 miles). This latency also depends on the network service level agreement (SLA) in terms of the bandwidth of the ISL links, packet drop rate, and jitter on the network. Low bandwidth, high jitter, and random packet drops lead to different recovery mechanisms by the switches or the TCP engine on the controller modules for successful packet delivery. These recovery mechanisms can increase overall latency.

  Any device that contributes to latency must be accounted for.

- Packet loss must be less than or equal to 0.01%.

  Packet loss includes physical loss or loss due to congestion or over-subscription.

  Packet drops can cause retransmissions and a reduced congestion window.

- The supported jitter value is 3 ms for round trip (or 1.5 ms for one way).
- The network should allocate and maintain the SLA for the bandwidth required for MetroCluster traffic, accounting for microbursts and spikes in the traffic.

  Low bandwidth can cause queuing delays and tail drops on switches. If you are using ONTAP 9.7 or later, the network intermediate between the two sites must provide a minimum bandwidth of 4.5 Gbps for the MetroCluster configuration.

- MetroCluster traffic should not consume the complete bandwidth and have negative impact on non-MetroCluster traffic.
- The shared network should have network monitoring configured to monitor the ISLs for utilization, errors (drops, link flaps, corruption, etc.) and failures.

Connection limits and trunking in the customer switches

The intermediate customer-provided switches must meet the following requirements:

- The number of intermediate switches is not limited, and more than two switches between the MetroCluster IP switches is supported.

  The MetroCluster IP switches should be located as close as possible to the intermediate switches providing the long-haul link. All of the ISL connections along the route must meet all of the requirements for MetroCluster ISL.

- The ISLs in the customer network (the ISLs between the customer switches) must be configured in such way that sufficient bandwidth is provided and order of delivery is preserved.

  This can be done with trunking a sufficient number of links and enforcing load balancing policies to preserve order.

Other network requirements

The intermediate customer-provided switches must meet the following requirements:

- The customer network must provide the same VLANs between the sites matching the MetroCluster VLANs as set in the RCF file.

  Layer 2 VLANs with IDs that match the MetroCluster VLAN IDs must span the shared network.

  - In ONTAP 9.7 and earlier, FAS2750 and AFF A220 systems require VLAN 10 and 20.
  - In ONTAP 9.8 and later, FAS2750, AFF A220, FAS500f, AFF A250, FAS8300, AFF A400, and FAS8700 systems use VLAN 10 and 20 by default. You can configure other VLANs during interface creation, and they must be withing the range 101-4096. For all the platforms mentioned previously, you can only specify the VLAN during interface creation. Once the MetroCluster interfaces are created, the VLAN ID cannot not be changed. For all other platforms not mentioned previously, you can use any VLAN and you can change the VLAN ID for those platforms at any time, but it requires that a new RCF file is created and applied.

> The RcfFileGenerator does not allow the creation of an RCF file using VLANs that are not supported by the platform.
>
> The RcfFileGenerator might restrict the use of certain VLAN IDs (for example, if they are intended for future use). Generally, reserved VLANs are up to and including 100.

- The MTU size must be set to 9216 on all devices in the end-to-end network.
- No other traffic can be configured with a higher priority than class of service (COS) five.
- ECN (explicit congestion notification) must be configured on all end-to-end paths.

Cabling requirements when using shared ISLs

When using shared ISLs in a MetroCluster IP configuration, you must be aware of the requirements for the end-to-end MetroCluster ISL running from controller ports on site A to controller ports on site B.

> You must follow the Basic MetroCluster ISL requirements.

Number of ISLs and breakout cables in the shared network

The number of ISLs connecting the MetroCluster IP switches to the shared network varies depending on the switch model and port type.

MetroCluster IP switch model	Port type	Number of ISLs
Broadcom-supported BES-53248 switches	Native ports	4 ISLs using 10 or 25-Gbps ports
Cisco 3132Q-V	Native ports	6 ISLs using 40-Gbps ports
Cisco 3132Q-V	Breakout cables	16 x 10-Gbps ISLs

Cisco 3232C	Native ports	6 ISLs using 40 or 100-Gbps ports
Cisco 3232C	Breakout cables	16 x 10-Gbps ISLs

- The use of breakout cables (one physical port is used as 4 x 10 Gbps ports) is supported on Cisco switches.
- The RCF files for the IP switches have ports in native and breakout mode configured.

  A mix of ISL ports in native port speed mode and breakout mode is not supported. All ISLs from the MetroCluster IP switches to the intermediate switches in one network must be of same speed and length.

- The use of external encryption devices (for example, external link encryption or encryption provided via WDM devices) are supported as long as the round-trip latency remains within the above requirements.

For optimum performance, you should use at least a 1 x 40 Gbps or multiple 10 Gbps ISLs per network. Using a single 10 Gbps ISL per network for AFF A800 systems is strongly discouraged.

The maximum theoretical throughput of shared ISLs (for example, 240 Gbps with six 40 Gbps ISLs) is a best-case scenario. When using multiple ISLs, statistical load balancing can impact the maximum throughput. Uneven balancing can occur and reduce throughput to that of a single ISL.

If the configuration uses L2 VLANs, they must natively span the sites. VLAN overlay such as Virtual Extensible LAN (VXLAN) is not supported.

ISLs carrying MetroCluster traffic must be native links between the switches. Link sharing services such as Multiprotocol Label Switching (MPLS) links are not supported.

Support for WAN ISLs on the Broadcom BES-53248 switch

- Minimum number of WAN ISLs per fabric: 1 (10 GbE, or 25 GbE, or 40 GbE, or 100 GbE)
- Maximum number of 10-GbE WAN ISLs per fabric: 4
- Maximum number of 25-GbE WAN ISLs per fabric: 4
- Maximum number of 40-GbE WAN ISLs per fabric: 2
- Maximum number of 100-GbE WAN ISLs per fabric: 2

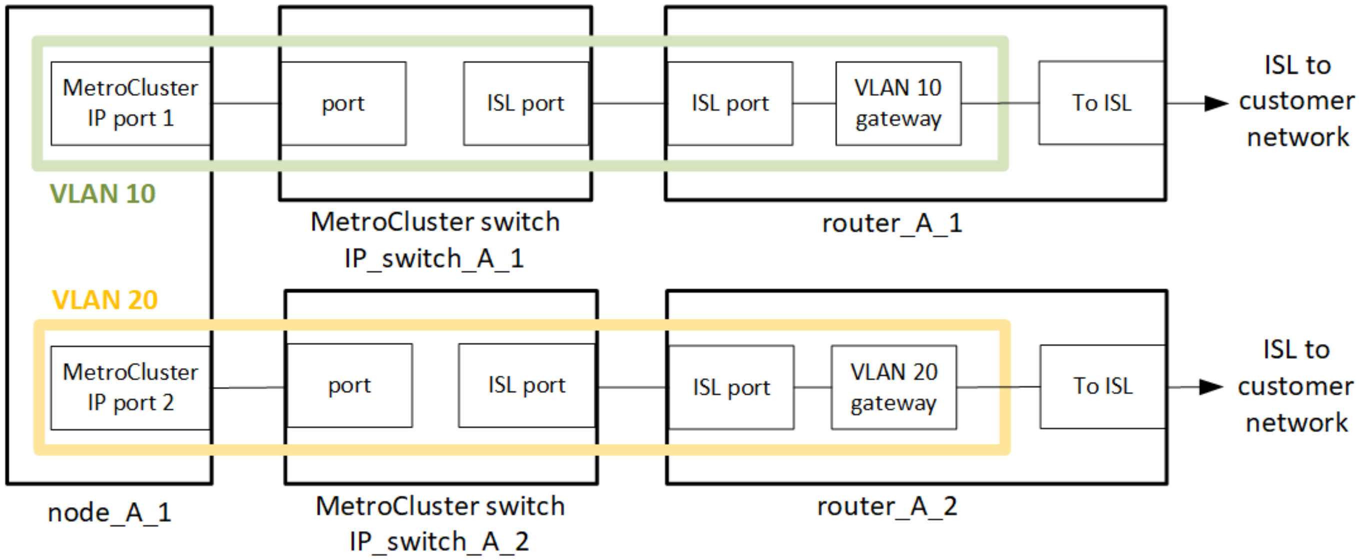
A 40-GbE or 100-GbE WAN ISL requires an RCF file version 1.40 or higher.

> Extra licenses are required for additional ports.

Considerations for layer 3 wide-area networks

Starting with ONTAP 9.9.1, MetroCluster IP configurations can be implemented with IP-routed (layer 3) backend connections.

The MetroCluster backend switches are connected to the routed IP network, either directly to routers (as shown in the following simplified example) or through other intervening switches.



NetApp supports only NetApp-validated switches. These switches are tested and sold by NetApp. They are listed in the NetApp Interoperability Matrix Tool (IMT) and in Cabling the IP switches.

The MetroCluster environment is configured and cabled as a standard MetroCluster IP configuration as described in Configure the MetroCluster hardware components. When you perform the installation and cabling procedure, you must perform the steps specific to the layer 3 configuration:

- The MetroCluster switches can be connected directly to the router or to one or more intervening switches. The VLAN must be extended to the gateway device.
- You use the `-gateway` parameter to configure the MetroCluster IP (MCC-IP) interface address with an IP gateway address.

When you configure routers and gateway IP addresses, ensure the following requirements are met:

- On each node, two interfaces cannot have the same gateway IP address.
- The corresponding interfaces on the HA pairs on each site must have the same gateway IP address.
- The corresponding interfaces on a node and its DR and AUX partners cannot have the same gateway IP address.
- The corresponding interfaces on a node and its DR and AUX partners must have the same VLAN ID.

The MetroCluster VLANs must extend from the edge MetroCluster switch to the gateway router so that MetroCluster traffic reaches the gateway (refer to the diagram shown above). The VLAN IDs for the MetroCluster VLANs must be the same at each site. However, the subnets can be different.

You use the RCF files that are created by the RcfFileGenerator tool. The network between the MetroCluster nodes and the gateway router must provide the same VLAN IDs as set in the RCF file.

IP-routed network requirements

The IP-routed network must meet the following requirements:

- Basic MetroCluster ISL requirements
- ISL requirements in shared layer 2 networks

* Required settings on intermediate switches
* Dynamic routing is not supported for the MetroCluster traffic.
* Only four-node MetroCluster configurations are supported (two nodes at each site).
* Two subnets are required on each MetroCluster site—one in each network.
* Auto-IP assignment is not supported.

Considerations for sharing private layer 2 networks

Starting with ONTAP 9.6, MetroCluster IP configurations with supported Cisco switches can share existing networks for ISLs, rather than using dedicated MetroCluster ISLs. Earlier ONTAP versions require dedicated ISLs.

MetroCluster IP switches are dedicated to the MetroCluster configuration and cannot be shared. Therefore, a set of MetroCluster IP switches can only connect one MetroCluster configuration. Only the MetroCluster ISL ports on the MetroCluster IP switches can connect to the shared switches.

> If using a shared network, the customer is responsible for meeting the MetroCluster network requirements in the shared network.

ISL requirements

You must meet the requirements in:

* Basic MetroCluster ISL requirements
* ISL requirements in shared layer 2 networks

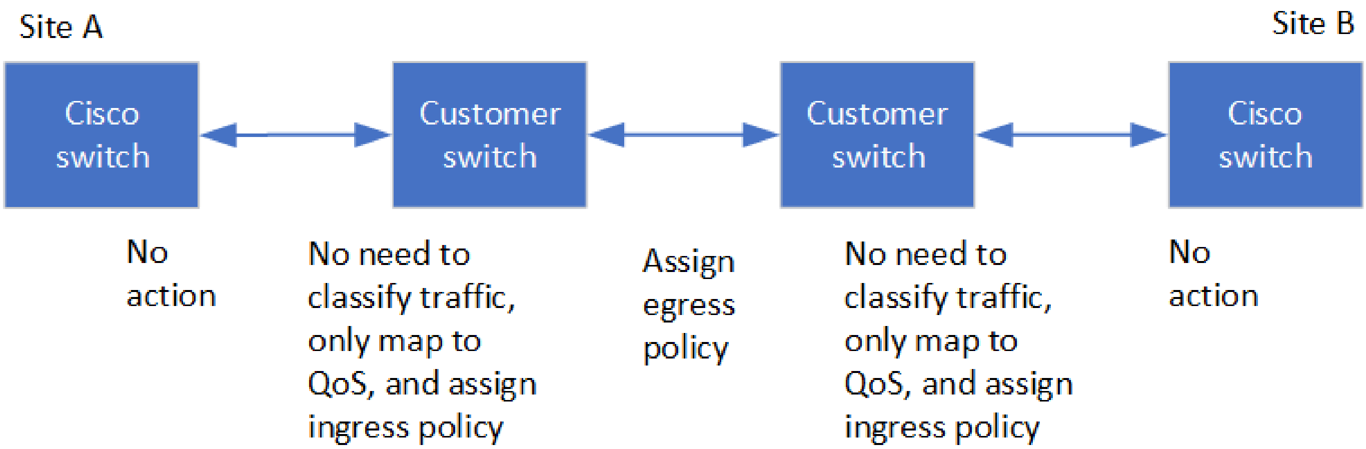
Required settings on intermediate switches

When sharing ISL traffic in a shared network, the configuration of the intermediate switches provided by the customer must ensure that the MetroCluster traffic (RDMA and storage) meets the required service levels across the entire path between the MetroCluster sites.

The following examples are for Cisco Nexus 3000 switches and IP Broadcom switches. Depending on your switch vendor and models, you must ensure that your intermediate switches have an equivalent configuration.

Cisco Nexus switches

The following diagram gives an overview of the required settings for a shared network when the external switches are Cisco switches.



In this example, the following policies and maps are created for MetroCluster traffic:

- A MetroClusterIP_Ingress policy is applied to ports on the intermediate switch that connect to the MetroCluster IP switches.

  The MetroClusterIP_Ingress policy maps the incoming tagged traffic to the appropriate queue on the intermediate switch. Tagging happens on the node-port, not on the ISL. Non-MetroCluster traffic that is using the same ports on the ISL remains in the default queue.

- A MetroClusterIP_Egress policy is applied to ports on the intermediate switch that connect to ISLs between intermediate switches

You must configure the intermediate switches with matching QoS access-maps, class-maps, and policy-maps along the path between the MetroCluster IP switches. The intermediate switches map RDMA traffic to COS5 and storage traffic to COS4.

The following example shows the configuration for a customer-provided Cisco Nexus 3000 switch. If you have Cisco switches, you can use the example to configure the switch along the path without much difficulty. If you do not have Cisco switches, you must determine and apply the equivalent configuration to your intermediate switches.

The following example shows the class map definitions:

> ⓘ This example is for configurations using Cisco MetroCluster IP switches. You can follow this example regardless of the switch types of the switches carrying MetroCluster traffic that do not connect to a MetroCluster IP switch.

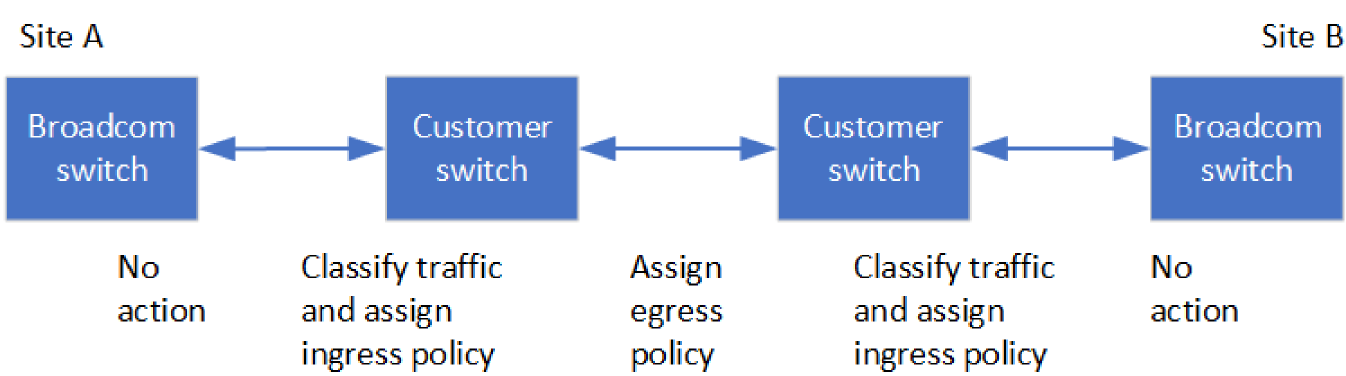
```
class-map type qos match-all rdma
   match cos 5
class-map type qos match-all storage
   match cos 4
```

The following example shows the policy map definitions:

```
policy-map type qos MetroClusterIP_Ingress
   class rdma
      set dscp 40
      set cos 5
      set qos-group 5
   class storage
      set dscp 32
      set cos 4
      set qos-group 4
policy-map type queuing MetroClusterIP_Egress
   class type queuing c-out-8q-q7
      priority level 1
   class type queuing c-out-8q-q6
      priority level 2
   class type queuing c-out-8q-q5
      priority level 3
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q4
      priority level 4
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q3
      priority level 5
   class type queuing c-out-8q-q2
      priority level 6
   class type queuing c-out-8q-q1
      priority level 7
   class type queuing c-out-8q-q-default
      bandwidth remaining percent 100
      random-detect threshold burst-optimized ecn
```

MetroCluster IP Broadcom switches

The following diagram gives an overview of the required settings for a shared network when the external switches are IP Broadcom switches.



Configurations using MetroCluster IP Broadcom switches require additional configuration:

- For exterior switches you must configure the access and class maps to classify the traffic on ingress to the customer network.

  > This is not required on configurations using MetroCluster IP switches.

  The following example shows how to configure the access and class maps on the first and last customer switches connecting the ISLs between the MetroCluster IP Broadcom switches.

```
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006

class-map type qos match-all storage
  match access-group name storage
class-map type qos match-all rdma
  match access-group name rdma
```

- You need to assign the ingress policy to the ISL switch port on the first customer switch.

  The following example shows the class map definitions:

  > This example is for configurations using Cisco MetroCluster IP switches. You can follow this example regardless of the switch types of the switches carrying MetroCluster traffic that do not connect to a MetroCluster IP switch.

```
class-map type qos match-all rdma
   match cos 5
class-map type qos match-all storage
   match cos 4
```

  The following example shows the policy map definitions:

```
policy-map type qos MetroClusterIP_Ingress
   class rdma
      set dscp 40
      set cos 5
      set qos-group 5
   class storage
      set dscp 32
      set cos 4
      set qos-group 4
policy-map type queuing MetroClusterIP_Egress
   class type queuing c-out-8q-q7
      priority level 1
   class type queuing c-out-8q-q6
      priority level 2
   class type queuing c-out-8q-q5
      priority level 3
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q4
      priority level 4
      random-detect threshold burst-optimized ecn
   class type queuing c-out-8q-q3
      priority level 5
   class type queuing c-out-8q-q2
      priority level 6
   class type queuing c-out-8q-q1
      priority level 7
   class type queuing c-out-8q-q-default
      bandwidth remaining percent 100
      random-detect threshold burst-optimized ecn
```

Intermediate customer switches

- For intermediate customer switches, you must assign the egress policy to the ISL switch ports.
- For all other interior switches along the path that carry MetroCluster traffic, follow the class map and policy map examples in the section *Cisco Nexus 3000 switches*.

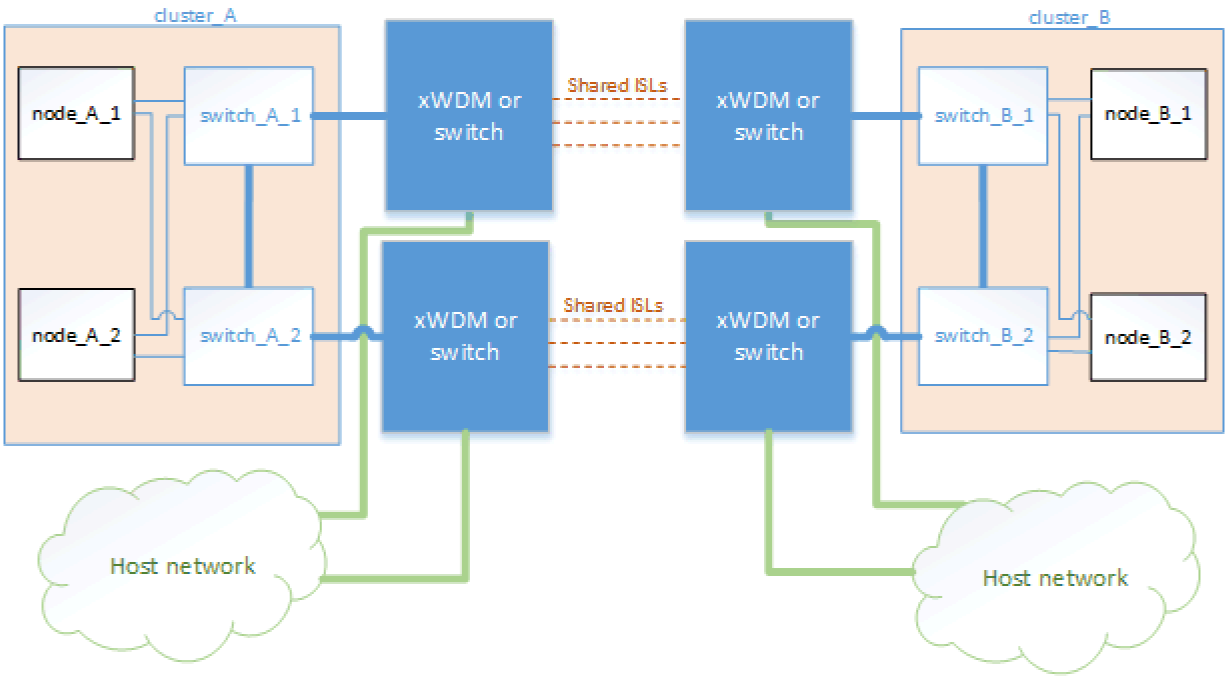
Examples of MetroCluster network topologies

Starting with ONTAP 9.6, some shared ISL network configurations are supported for MetroCluster IP configurations.

Shared network configuration with direct links

In this topology, two distinct sites are connected by direct links. These links can be between Wavelength Division Multiplexing equipment (xWDM) or switches. The capacity of the ISLs is not dedicated to the MetroCluster traffic but is shared with other traffic.

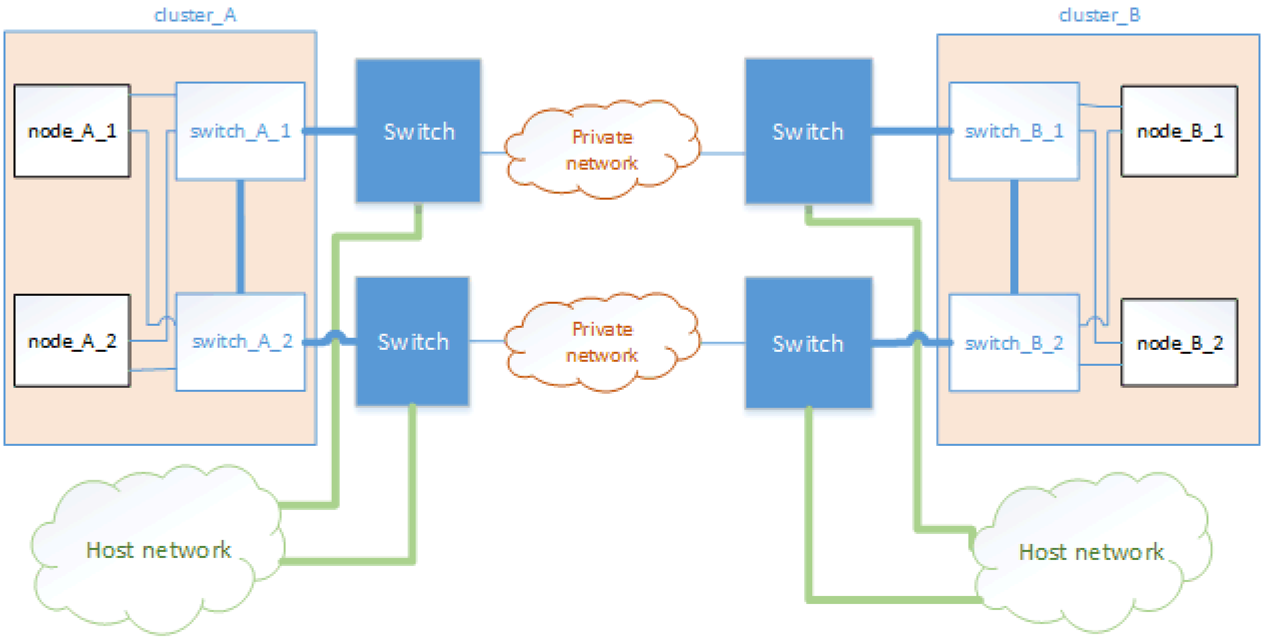
The ISL capacity must meet the minimum requirements. Depending on whether you use xWDM devices or switches a different combination of network configurations might apply.



Shared infrastructure with intermediate networks

In this topology, the MetroCluster IP core switch traffic and the host traffic travel through a network that is not provided by NetApp. The network infrastructure and the links (including leased direct links) are outside of the MetroCluster configuration. The network can consist of a series of xWDM and switches but unlike the shared configuration with direct ISLs, the links are not direct between the sites. Depending on the infrastructure between the sites, any combination of network configurations is possible. The intermediate infrastructure is represented as a “cloud” (multiple devices can exist between the sites), but it is still under the control of the customer. Capacity through this intermediate infrastructure is not dedicated to the MetroCluster traffic but is shared with other traffic.

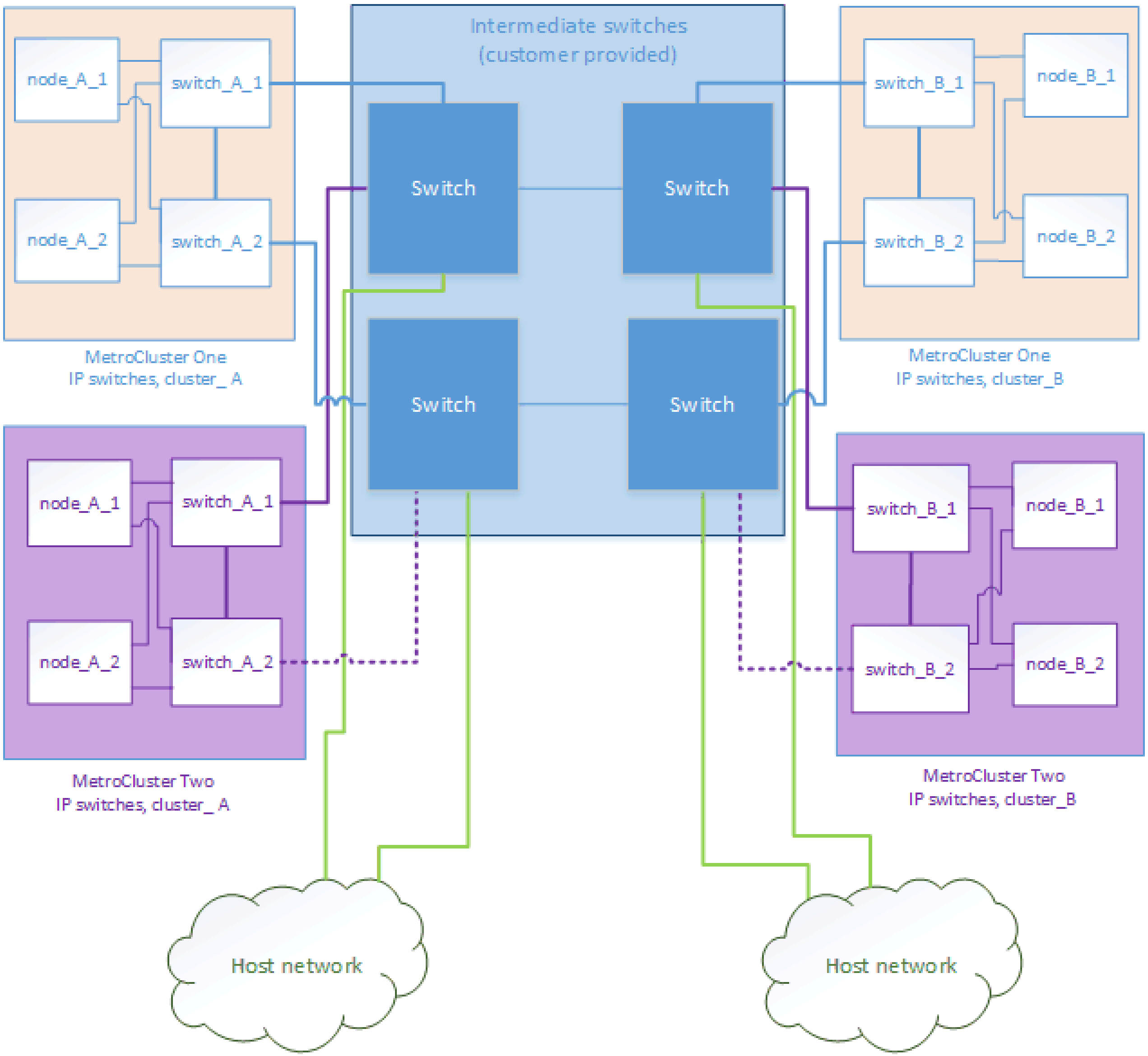
The VLAN and network xWDM or switch configuration must meet the minimum requirements.



Two MetroCluster configurations sharing an intermediate network

In this topology, two separate MetroCluster configurations are sharing the same intermediate network. In the example, MetroCluster one switch_A_1 and MetroCluster two switch_A_1 both connect to the same intermediate switch.

The example is simplified for illustration purposes only:



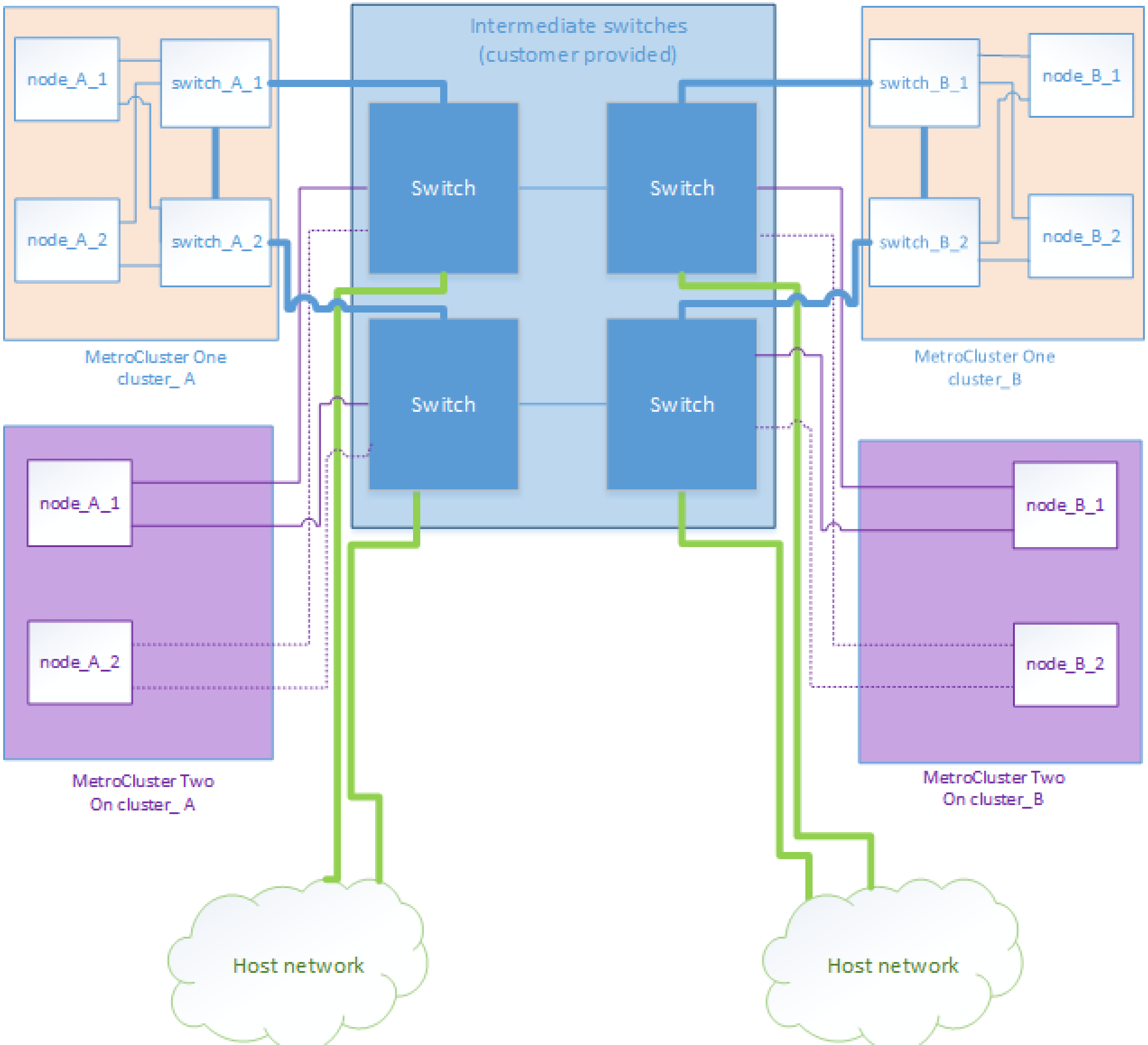
Two MetroCluster configurations with one connecting directly to the intermediate network

This topology is supported beginning with ONTAP 9.7. Two separate MetroCluster configurations share the same intermediate network and one MetroCluster configuration's nodes is directly connected to the intermediate switch.

MetroCluster One is a MetroCluster configuration using NetApp validated switches, ONTAP 9.6 and a shared topology. MetroCluster Two is a MetroCluster configuration using NetApp-compliant switches and ONTAP 9.7.

> The intermediate switches must be compliant with NetApp specifications.

The example is simplified for illustration purposes only:



Considerations for using MetroCluster-compliant switches

MetroCluster IP switches provided by NetApp are NetApp-validated. Beginning with ONTAP 9.7, MetroCluster IP configurations can support switches that are not NetApp-validated provided that they are compliant with NetApp specifications.

General requirements

The requirements show how to configure MetroCluster-compliant switches without using reference configuration (RCF) files.

- Only platforms that provide dedicated ports for switchless cluster interconnects are supported. Platforms such as FAS2750 and AFF A220 are not supported because MetroCluster traffic and MetroCluster interconnect traffic share the same network ports.

  Connecting local cluster connections to a MetroCluster-compliant switch is not supported.

- The MetroCluster IP interface can be connected to any switch port that can be configured to meet the requirements.

- The speed of the switch ports must be 25 Gbps for FAS8200 and AFF A300 platforms, and at least 40 Gbps for all other platforms (40 Gbps or 100 Gbps).
- The ISLs must be 10 Gbps or higher and must be sized appropriately for the load on the MetroCluster configuration.
- The MetroCluster configuration must be connected to two networks. Connecting both the MetroCluster interfaces to the same network or switch is not supported. Each MetroCluster node must be connected to two network switches.
- The network must meet the following requirements:
  - Basic MetroCluster ISL requirements
  - ISL requirements in shared layer 2 networks
  - Required settings on intermediate switches
- In MetroCluster IP configurations using open networks, reverting to ONTAP 9.6 or earlier is not supported.
- The MTU of 9216 must be configured on all switches that carry MetroCluster IP traffic.

Switch and cabling requirements

- The switches must support QoS/traffic classification.
- The switches must support explicit congestion notification (ECN).
- The switches must support L4 port-vlan load-balancing policies to preserve order along the path.
- The switches must support L2 Flow Control (L2FC).
- The cables connecting the nodes to the switches must be purchased from NetApp. The cables we provide must be supported by the switch vendor.

Limitations

Any configuration or feature that requires that the local cluster connections are connected to a switch is not supported. For example, the following configurations and procedures are not supported:

- Eight-node MetroCluster configurations
- Transitioning from MetroCluster FC to MetroCluster IP configurations
- Refreshing a four-node MetroCluster IP configuration

Platform-specific network speeds for MetroCluster-compliant switches

The following table provides platform-specific network speeds for MetroCluster compliant switches.

Missing values indicate that the platform is not supported.

Platform	Network Speed (Gbps)
AFF A800	40 or 100
AFF A700	40
AFF A400	100

AFF A320	100
AFF A300	25
AFF A250	-
AFF A220	-
FAS9000	40
FAS8700	100
FAS8300	100
FAS8200	25
FAS2750	-
FAS500f	-

Assumptions for the examples

The examples provided are valid for Cisco NX31xx and NX32xx switches. If other switches are used, these commands can be used as guidance, but the commands might be different. If a feature shown in the examples is not available on the switch, this means that the switch does not meet the minimum requirements and cannot be used to deploy a MetroCluster configuration. This is true for any switch that is connecting a MetroCluster configuration and for all switches on the path between those switches.

- The ISL ports are 15 and 16 and operate at a speed of 40 Gbps.
- The VLAN in network 1 is 10 and the VLAN in network 2 is 20. Examples might be shown for one network only.
- The MetroCluster interface is connected to port 9 on each switch and operates at a speed of 100 Gbps.
- The full context of the examples is not set or shown. You might need to enter further configuration information such as the profile, VLAN, or interface, to execute the commands.

Generic switch configuration

A VLAN in each network must be configured. The example shows how to configure a VLAN in network 10.

Example:

```
# vlan 10
```

The load balancing policy should be set so that order is preserved.

Example:

```
# port-channel load-balance src-dst ip-l4port-vlan
```

You must configure the access and class maps, which map the RDMA and iSCSI traffic to the appropriate classes.

All TCP traffic to and from the port 65200 is mapped to the storage (iSCSI) class. All TCP traffic to and from the port 10006 is mapped to the RDMA class.

Example:

```
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006

class-map type qos match-all storage
  match access-group name storage
class-map type qos match-all rdma
  match access-group name rdma
```

You must configure the ingress policy. The ingress policy maps the traffic as classified to the different COS groups. In this example, the RDMA traffic is mapped to COS group 5 and iSCSI traffic is mapped to COS group 4.

Example:

```
policy-map type qos MetroClusterIP_Ingress
class rdma
  set dscp 40
  set cos 5
  set qos-group 5
class storage
  set dscp 32
  set cos 4
  set qos-group 4
```

You must configure the egress policy on the switch. The egress policy maps the traffic to the egress queues. In this example, RDMA traffic is mapped to queue 5 and iSCSI traffic is mapped to queue 4.

Example:

```
policy-map type queuing MetroClusterIP_Egress
class type queuing c-out-8q-q7
  priority level 1
class type queuing c-out-8q-q6
  priority level 2
class type queuing c-out-8q-q5
  priority level 3
  random-detect threshold burst-optimized ecn
class type queuing c-out-8q-q4
  priority level 4
  random-detect threshold burst-optimized ecn
class type queuing c-out-8q-q3
  priority level 5
class type queuing c-out-8q-q2
  priority level 6
class type queuing c-out-8q-q1
  priority level 7
class type queuing c-out-8q-q-default
  bandwidth remaining percent 100
  random-detect threshold burst-optimized ecn
```

You need to configure a switch that has MetroCluster traffic on an ISL but does not connect to any MetroCluster interfaces. In this case, the traffic is already classified and only needs to be mapped to the appropriate queue. In the following example, all of the COS5 traffic is mapped to the class RDMA, and all of the COS4 traffic is mapped to the class iSCSI. Note that this will affect **all** of the COS5 and COS4 traffic, not only the MetroCluster traffic. If you only want to map the MetroCluster traffic, then you must use the above class maps to identify the traffic using the access groups.

Example:

```
class-map type qos match-all rdma
  match cos 5
class-map type qos match-all storage
  match cos 4
```

Configuring the ISLs

You can configure a 'trunk' mode port when setting an allowed VLAN.

There are two commands, one to **set** the allowed VLAN list, and one to **add** to the existing allowed VLAN list.

You can **set** the allowed VLANs as shown in the example.

Example:

```
switchport trunk allowed vlan 10
```

You can **add** a VLAN to the allowed list as shown in the example.

Example:

```
switchport trunk allowed vlan add 10
```

In the example, port-channel 10 is configured for VLAN 10.

Example:

```
interface port-channel10
switchport mode trunk
switchport trunk allowed vlan 10
mtu 9216
service-policy type queuing output MetroClusterIP_Egress
```

The ISL ports should be configured as part of a port-channel and be assigned the egress queues as shown in the example.

Example:

```
interface eth1/15-16
switchport mode trunk
switchport trunk allowed vlan 10
no lldp transmit
no lldp receive
mtu 9216
channel-group 10 mode active
service-policy type queuing output MetroClusterIP_Egress
no shutdown
```

Configuring the node ports

You might need to configure the node port in breakout mode. In this example, ports 25 and 26 are configured in 4 x 25 Gbps breakout mode.

Example:

```
interface breakout module 1 port 25-26 map 25g-4x
```

You might need to configure the MetroCluster interface port speed. The example shows how to configure the speed to "auto".

Example:

```
speed auto
```

The following example shows how to fix the speed at 40 Gbps.

Example:

```
speed 40000
```

You might need to configure the interface. In the following example, the interface speed is set to "auto".

The port is in access mode in VLAN 10, MTU is set to 9216 and the MetroCluster ingress policy is assigned.

Example:

```
interface eth1/9
description MetroCluster-IP Node Port
speed auto
switchport access vlan 10
spanning-tree port type edge
spanning-tree bpduguard enable
mtu 9216
flowcontrol receive on
flowcontrol send on
service-policy type qos input MetroClusterIP_Ingress
no shutdown
```

On 25-Gbps ports, the FEC setting might need to be set to "off" as shown in the example.

Example:

```
fec off
```

> You must always run this command **after** the interface is configured. A transceiver module might need to be inserted for the command to work.

Using TDM/xWDM and encryption equipment with MetroCluster IP configurations

You should be aware of certain considerations for using multiplexing equipment in the MetroCluster IP configuration.

These considerations apply only to direct, dedicated MetroCluster back-end links and switches, not links shared with non-MetroCluster traffic.

The Hardware Universe tool provides some notes about the requirements that TDM/xWDM equipment must meet to work with a MetroCluster IP configuration.

NetApp Hardware Universe

Using encryption on WDM or external encryption devices

When using encryption on WDM devices in the MetroCluster IP configuration, your environment must meet the following requirements:

- The external encryption devices or DWDM equipment must have been certified by the vendor with the switch in question.

  The certification should cover the operating mode (such as trunking and encryption).

- The overall end-to-end latency and jitter, including the encryption, cannot be above the maximum stated in the IMT or in this document.

SFP considerations

Any SFPs or QSFPs supported by the equipment vendor are supported for the MetroCluster ISLs. SFPs and QSFPs can be acquired from NetApp or the equipment vendor.

Considerations for ISLs

The ISLs on one fabric should all be the same speed and length.

The ISLs on one fabric should all have the same topology. For example, they should all be direct links, or if the configuration uses WDM, then they should all use WDM.

If you are sharing ISLs with a non-MetroCluster network, you must follow the guidelines in the section Considerations for sharing private layer 2 networks.

The maximum supported difference in distance between fabric 1 and fabric 2 is 20 km.

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 are 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 metadata volume and data SVM root volumes

The configuration replication service (CRS) metadata volume and data SVM 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

SVMs 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.

Considerations for unmirrored aggregates and SAN

Prior to ONTAP 9.9.1, a LUN should not be located on an unmirrored aggregate. Configuring a LUN on an unmirrored aggregate can result in a switchover operation that exceeds 120 seconds and a data outage.

Considerations for adding storage shelves for unmirrored aggregates

> If you are adding shelves that will be used for unmirrored aggregates in a MetroCluster IP configuration, you must do the following:

1. Before starting the procedure to add the shelves, issue the following command:

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment true
   ```

2. Verify that automatic disk assignment is off:

   ```
   disk option show
   ```

3. Follow the steps of the procedure to add the shelf.
4. Manually assign all disks from new shelf to the node that will own the unmirrored aggregate or aggregates.
5. Create the aggregates:

   ```
   storage aggregate create
   ```

6. After completing the procedure, issue the following command:

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment false
   ```

7. Verify that automatic disk assignment is enabled:

   ```
   disk option show
   ```

Firewall usage at MetroCluster sites

If you are using a firewall at a MetroCluster site, you must ensure access for certain required ports.

Considerations for firewall usage at MetroCluster sites

If you are using a firewall at a MetroCluster site, you must ensure access for required ports.

The following table shows TCP/UDP port usage in an external firewall positioned between two MetroCluster sites.

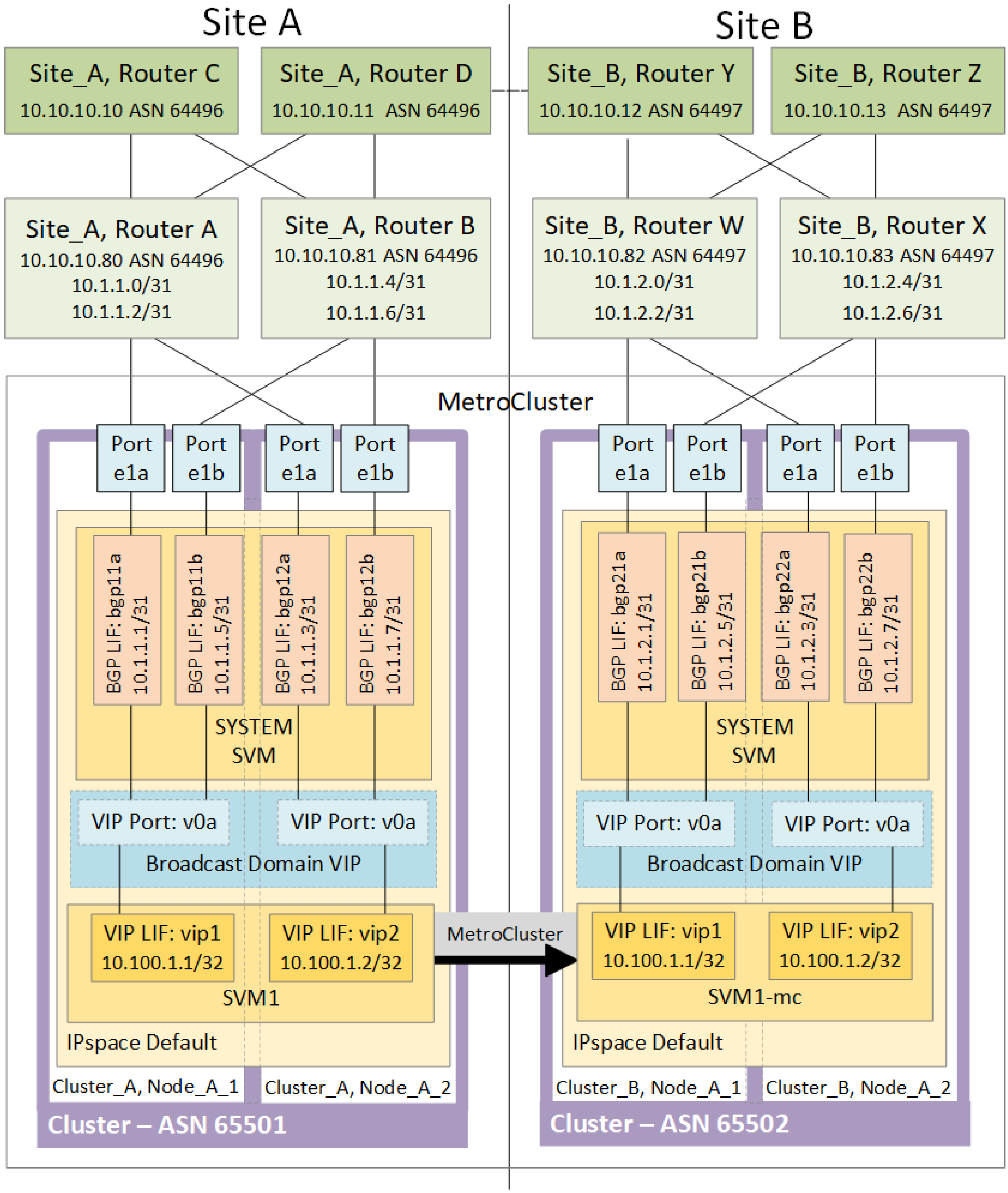
Traffic type	Port/services
Cluster peering	11104 / TCP 11105 / TCP
ONTAP System Manager	443 / TCP
MetroCluster IP intercluster LIFs	65200 / TCP 10006 / TCP and UDP
Hardware assist	4444 / TCP

Considerations for using virtual IP and Border Gateway Protocol with a MetroCluster configuration

Starting with ONTAP 9.5, ONTAP supports layer 3 connectivity using virtual IP (VIP) and Border Gateway Protocol (BGP). The combination VIP and BGP for redundancy in the front-end networking with the back-end MetroCluster redundancy provides a layer 3 disaster recovery solution.

Review the following guidelines and illustration when planning your layer 3 solution. For details on implementing VIP and BGP in ONTAP, refer to the following section:

Configuring virtual IP (VIP) LIFs



ONTAP limitations

ONTAP does not automatically verify that all nodes on both sites of the MetroCluster configuration are configured with BGP peering.

ONTAP does not perform route aggregation but announces all individual virtual LIF IPs as unique host routes at all times.

ONTAP does not support true AnyCast — only a single node in the cluster presents a specific virtual LIF IP (but is accepted by all physical interfaces, regardless of whether they are BGP LIFs, provided the physical port is part of the correct IPspace). Different LIFs can migrate independently of each other to different hosting nodes.

Guidelines for using this Layer 3 solution with a MetroCluster configuration

You must configure your BGP and VIP correctly to provide the required redundancy.

Simpler deployment scenarios are preferred over more complex architectures (for example, a BGP peering router is reachable across an intermediate, non-BGP router). However, ONTAP does not enforce network design or topology restrictions.

VIP LIFs only cover the frontend/data network.

Depending on your version of ONTAP, you must configure BGP peering LIFs in the node SVM, not the system or data SVM. In 9.8, the BGP LIFs are visible in the cluster (system) SVM and the node SVMs are no longer present.

Each data SVM requires the configuration of all potential first hop gateway addresses (typically, the BGP router peering IP address), so that the return data path is available if a LIF migration or MetroCluster failover occurs.

BGP LIFs are node specific, similar to intercluster LIFs — each node has a unique configuration, which does not need to be replicated to DR site nodes.

configured, the existence of the v0a (v0b and so on.) continuously validates the connectivity, guaranteeing that a LIF migrate or failover succeeds (unlike L2, where a broken configuration is only visible after the outage).

A major architectural difference is that clients should no longer share the same IP subnet as the VIP of data SVMs. An L3 router with appropriate enterprise grade resiliency and redundancy features enabled (for example, VRRP/HSRP) should be on the path between storage and clients for the VIP to operate correctly.

The reliable update process of BGP allows for smoother LIF migrations because they are marginally faster and have a lower chance of interruption to some clients

You can configure BGP to detect some classes of network or switch misbehaviors faster than LACP, if configured accordingly.

External BGP (EBGP) uses different AS numbers between ONTAP node(s) and peering routers and is the preferred deployment to ease route aggregation and redistribution on the routers. Internal BGP (IBGP) and the use of route reflectors is not impossible but outside the scope of a straightforward VIP setup.

After deployment, you must check that the data SVM is accessible when the associated virtual LIF is migrated between all nodes on each site (including MetroCluster switchover) to verify the correct configuration of the static routes to the same data SVM.

VIP works for most IP-based protocols (NFS, SMB, iSCSI).

Configuring the MetroCluster hardware components

The MetroCluster components must be physically installed, cabled, and configured at both geographic sites.

Parts of a MetroCluster IP configuration

As you plan your MetroCluster IP configuration, you should understand the hardware components and how they interconnect.

Key hardware elements

A MetroCluster IP configuration includes the following key hardware elements:

- Storage controllers

  The storage controllers are configured as two two-node clusters.

- IP network

  This back-end IP network provides connectivity for two distinct uses:

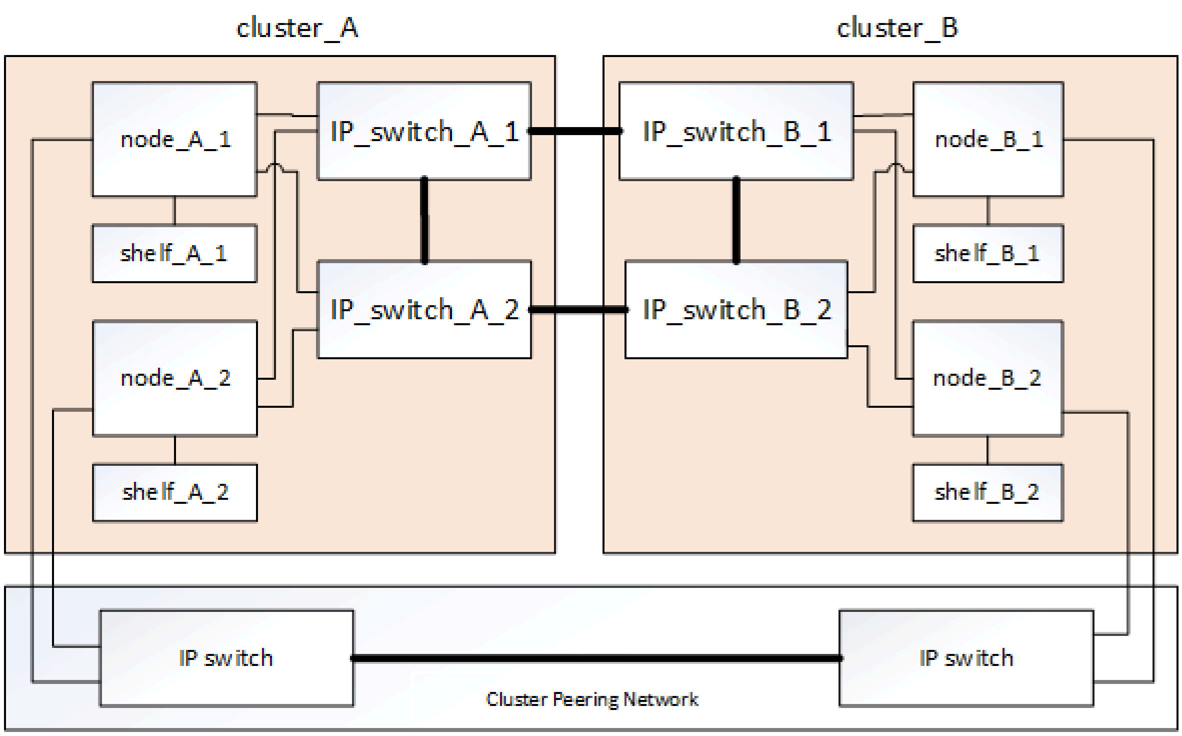
  - Standard cluster connectivity for intra-cluster communications.

    This is the same cluster switch functionality used in non-MetroCluster switched ONTAP clusters.

  - MetroCluster back-end connectivity for replication of storage data and non-volatile cache.

- Cluster peering network

  The cluster peering network provides connectivity for mirroring of the cluster configuration, which includes storage virtual machine (SVM) configuration. The configuration of all of the SVMs on one cluster is mirrored to the partner cluster.



Disaster Recovery (DR) groups

A MetroCluster IP configuration consists of one DR group of four nodes.

The following illustration shows the organization of nodes in a four-node MetroCluster configuration:

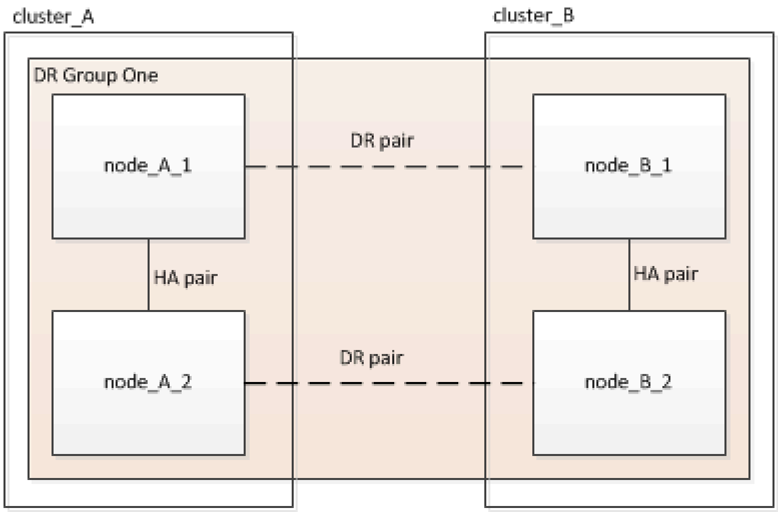
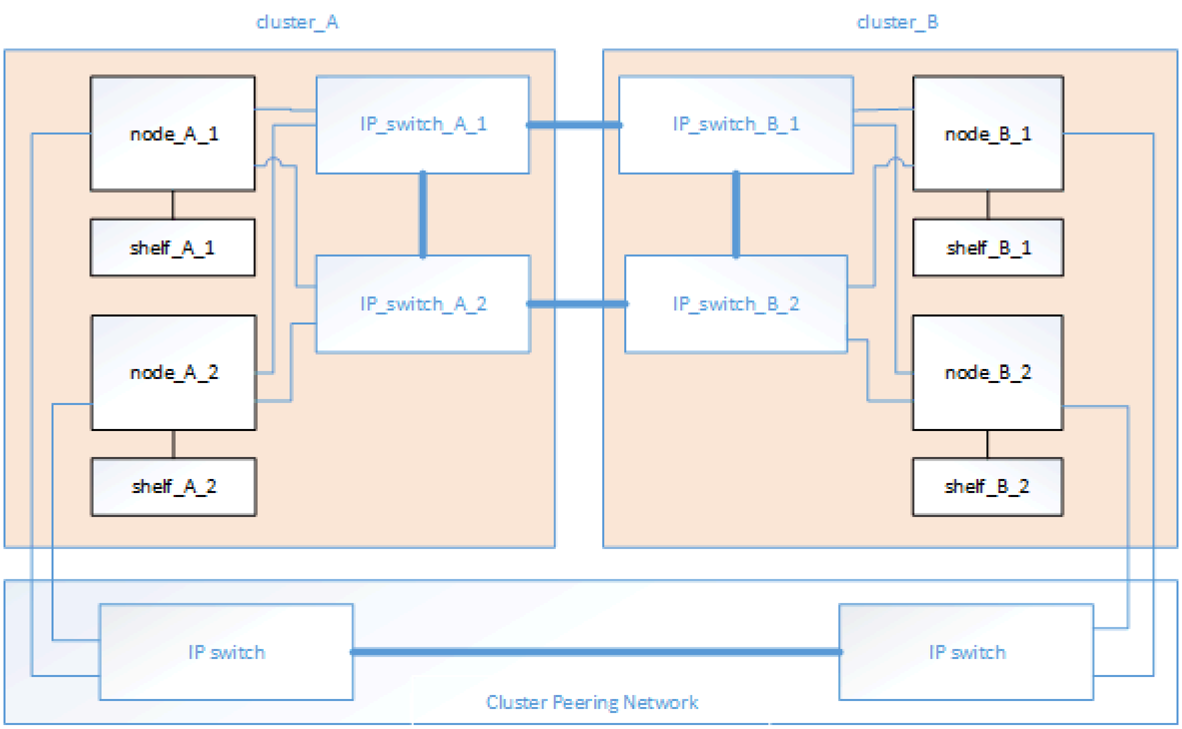


Illustration of the local HA pairs in a MetroCluster configuration

Each MetroCluster site consists of storage controllers configured as an HA pair. This allows local redundancy so that if one storage controller fails, its local HA partner can take over. Such failures can be handled without a MetroCluster switchover operation.

Local HA failover and giveback operations are performed with the storage failover commands, in the same manner as a non-MetroCluster configuration.

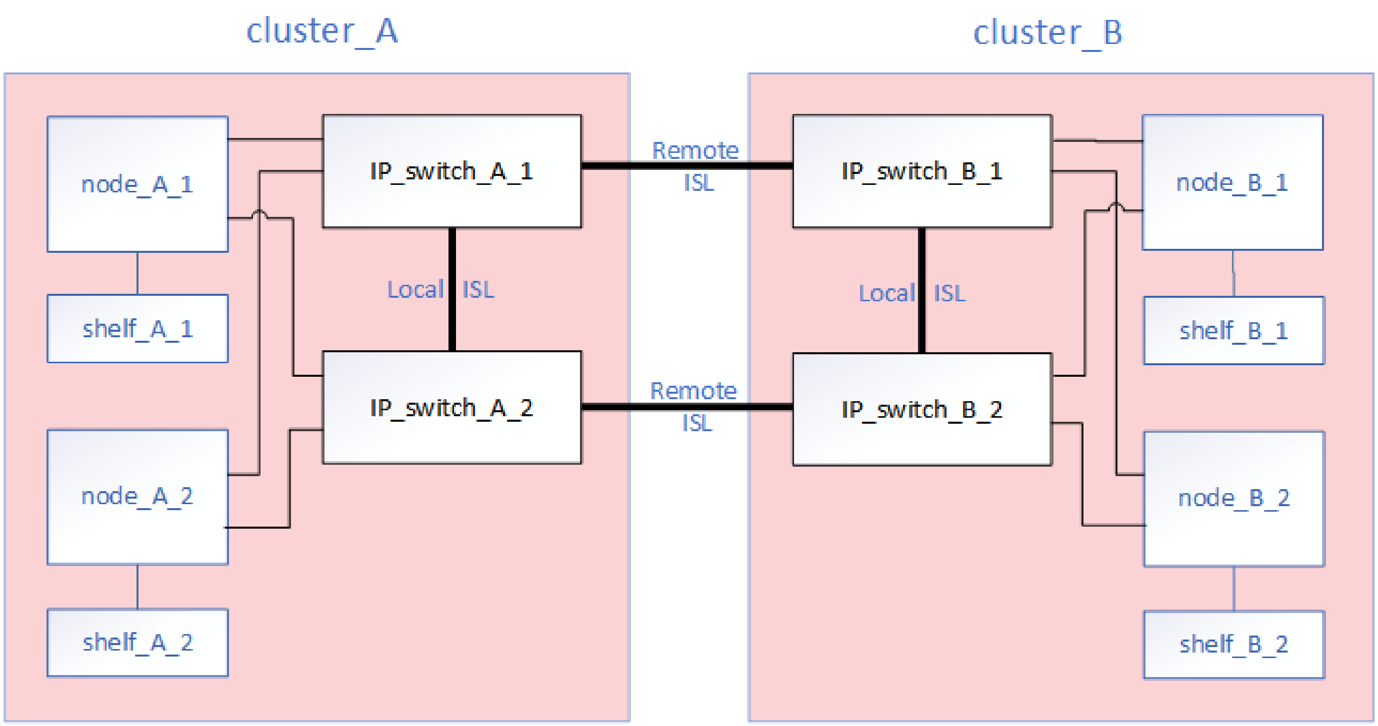


Related information

ONTAP concepts

Illustration of the MetroCluster IP and cluster interconnect network

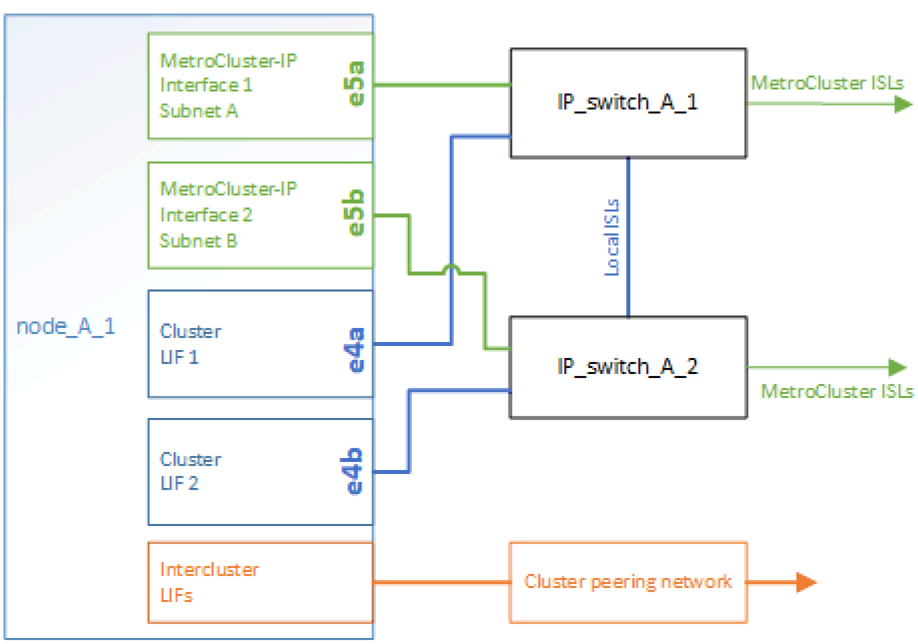
ONTAP clusters typically include a cluster interconnect network for traffic between the nodes in the cluster. In MetroCluster IP configurations, this network is also used for carrying data replication traffic between the MetroCluster sites.



Each node in the MetroCluster IP configuration has specialized LIFs for connection to the back-end IP network:

- Two MetroCluster IP interfaces
- One intercluster LIF

The following illustration shows these interfaces. The port usage shown is for an AFF A700 or FAS9000 system.



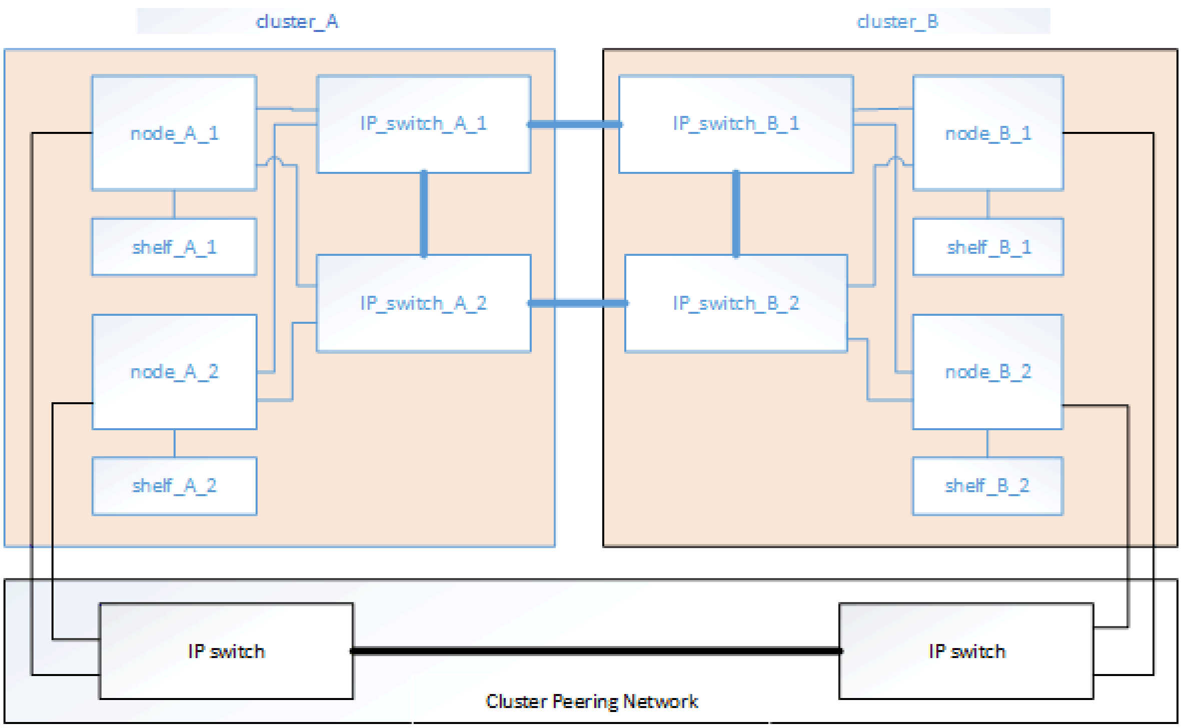
Related information

Considerations for MetroCluster IP configurations

Illustration of the cluster peering network

The two clusters in the MetroCluster configuration are peered through a customer-provided cluster peering network. Cluster peering supports the synchronous mirroring of storage virtual machines (SVMs, formerly known as Vservers) between the sites.

Intercluster LIFs must be configured on each node in the MetroCluster configuration, and the clusters must be configured for peering. The ports with the intercluster LIFs are connected to the customer-provided cluster peering network. Replication of the SVM configuration is carried out over this network through the Configuration Replication Service.



Related information

Cluster and SVM peering express configuration

Considerations for configuring cluster peering

Cabling the cluster peering connections

Peering the clusters

Required MetroCluster IP components and naming conventions

When planning your MetroCluster IP 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.

Supported software and hardware

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

NetApp Hardware Universe

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

Hardware redundancy requirements in a MetroCluster IP configuration

Because of the hardware redundancy in the MetroCluster IP 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.

ONTAP cluster requirements in a MetroCluster IP configuration

MetroCluster IP configurations require two ONTAP clusters, one at each MetroCluster site.

Naming must be unique within the MetroCluster configuration.

Example names:

- Site A: cluster_A
- Site B: cluster_B

IP switch requirements in a MetroCluster IP configuration

MetroCluster IP configurations require four IP switches. The four switches form two switch storage fabrics that provide the ISL between each of the clusters in the MetroCluster IP configuration.

The IP switches also provide intracluster communication among the controller modules in each cluster.

Naming must be unique within the MetroCluster configuration.

Example names:

- Site A: cluster_A
  - IP_switch_A_1
  - IP_switch_A_2
- Site B: cluster_B
  - IP_switch_B_1
  - IP_switch_B_2

Controller module requirements in a MetroCluster IP configuration

MetroCluster IP configurations require four or eight controller modules.

The controller modules at each site form an HA pair. Each controller module has a DR partner at the other site.

Each controller module must be running the same ONTAP version. Supported platform models depend on the ONTAP version:

* New MetroCluster IP installations on FAS systems are not supported in ONTAP 9.4.

  Existing MetroCluster IP configurations on FAS systems can be upgraded to ONTAP 9.4.
* Starting with ONTAP 9.5, new MetroCluster IP installations on FAS systems are supported.
* Starting with ONTAP 9.4, controller modules configured for ADP are supported.

Controller models limited to four-node configurations

These models are limited to four in a MetroCluster configuration.

* AFF A220
* AFF A250
* FAS2750
* FAS500f

For example, the following configurations are not supported:

* An eight-node configuration consisting of eight AFF A250 controllers.
* An eight-node configuration consisting of four AFF 220 controllers and four FAS500f controllers.
* Two four-node MetroCluster IP configurations each consisting of AFF A250 controllers and sharing the same back-end switches.
* An eight-node configuration consisting of DR Group 1 with AFF A250 controllers and DR Group 2 with FAS9000 controllers.

You can configure two separate four-node MetroCluster IP configurations with the same back-end switches if the second MetroCluster does not include any of the above models.

Example names

The following example names are used in the documentation:

* Site A: cluster_A
  * controller_A_1
  * controller_A_2
* Site B: cluster_B
  * controller_B_1
  * controller_B_2

Gigabit Ethernet adapter requirements in a MetroCluster IP configuration

MetroCluster IP configurations use a 40/100 Gbps or 10/25 Gbps Ethernet adapter for the IP interfaces to the IP switches used for the MetroCluster IP fabric.

Platform model	Required Gigabit Ethernet adapter	Required slot for adapter	Ports
AFF A700 and FAS9000	X91146A-C	Slot 5	e5a, e5b

AFF A800	X1146A/onboard ports	Slot 1	e0b. e1b
AFF A400 and FAS8300	X1146A	Slot 1	e1a, e1b
AFF A300 and FAS8200	X1116A	Slot 1	e1a, e1b
AFF A220, and FAS2750	Onboard ports	Slot 0	e0a, e0b
AFF A250 and FAS500f	Onboard ports	Slot 0	e0c, e0d
AFF A320	Onboard ports	Slot 0	e0g, e0h

Pool and drive requirements (minimum supported)

Eight SAS disk shelves are recommended (four shelves at each site) to allow disk ownership on a per-shelf basis.

A four-node MetroCluster IP configuration requires the minimum configuration at each site:

- Each node has at least one local pool and one remote pool at the site.
- At least seven drives in each pool.

  In a four-node MetroCluster configuration with a single mirrored data aggregate per node, the minimum configuration requires 24 disks at the site.

In a minimum supported configuration, each pool has the following drive layout:

- Three root drives
- Three data drives
- One spare drive

In a minimum supported configuration, at least one shelf is needed per site.

MetroCluster configurations support RAID-DP and RAID4.

Drive location considerations for partially populated shelves

For correct auto-assignment of drives when using shelves that are half populated (12 drives in a 24-drive shelf), drives should be located in slots 0-5 and 18-23.

In a configuration with a partially populated shelf, the drives must be evenly distributed in the four quadrants of the shelf.

Drive location considerations for AFF A800 internal drives

For correct implementation of the ADP feature, the AFF A800 system disk slots must be divided into quarters and the disks must be located symmetrically in the quarters.

An AFF A800 system has 48 drive bays. The bays can be divided into quarters:

- Quarter one:
  - Bays 0 - 5
  - Bays 24 - 29
- Quarter two:
  - Bays 6 - 11
  - Bays 30 - 35
- Quarter three:
  - Bays 12 - 17
  - Bays 36 - 41
- Quarter four:
  - Bays 18 - 23
  - Bays 42 - 47

If this system is populated with 16 drives, they must be symmetrically distributed among the four quarters:

- Four drives in the first quarter: 0, 1, 2, 3
- Four drives in the second quarter: 12, 13, 14, 15
- Four drives in the third quarter: 24, 25, 26, 27
- Four drives in the fourth quarter: 36, 37, 38, 39

Mixing IOM12 and IOM 6 modules in a stack

Your version of ONTAP must support shelf mixing. Refer to the NetApp Interoperability Matrix Tool (IMT) to see if your version of ONTAP supports shelf mixing.

For further details on shelf mixing, see Hot-adding shelves with IOM12 modules to a stack of shelves with IOM6 modules

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 controller modules, the switch types, and the number of disk shelf stacks in your configuration.

2. Properly ground yourself.

3. Install the controller modules in the rack or cabinet.

   AFF A220/FAS2700 Systems Installation and Setup Instructions

AFF A250 Systems Installation and Setup Instructions

AFF A300 Systems Installation and Setup Instructions

AFF A320 systems: Installation and setup

AFF A400 Systems Installation and Setup Instructions

AFF A700 Systems Installation and Setup Instructions

AFF A800 Systems Installation and Setup Instructions

FAS500f Systems Installation and Setup Instructions

FAS8200 Systems Installation and Setup Instructions

FAS8300 and FAS8700 Systems Installation and Setup Instructions

FAS9000 Systems Installation and Setup Instructions

4. Install the IP switches in the rack or cabinet.
5. Install the disk shelves, power them on, and then set the shelf IDs.
   - You must power-cycle each disk shelf.
   - Shelf IDs must be unique for each SAS disk shelf within each MetroCluster DR group (including both sites).

> Do not cable disk shelves intended to contain unmirrored aggregates at this time. You must wait to deploy shelves intended for unmirrored aggregates until after the MetroCluster configuration is complete and only deploy them after using the `metrocluster modify -enable-unmirrored-aggr-deployment true` command.

Cabling the IP switches

You must cable each IP switch to the local controller modules and to the ISLs.

- This task must be repeated for each switch in the MetroCluster configuration.
- The controller module Ethernet port usage depends on the model of the controller module.

Using the port tables with the RcfFileGenerator tool or multiple MetroCluster configurations

You must understand how to use the information in the port tables to correctly generate your RCF files.

Before you begin

Review these considerations before using the tables:

- The following tables show the port usage for site A. The same cabling is used for site B.
- The switches cannot be configured with ports of different speeds (for example, a mix of 100 Gbps ports and 40 Gbps ports).

* Keep track of the MetroCluster port group (MetroCluster 1, MetroCluster 2, etc.). You will need this information when using the RcfFileGenerator tool as described later in this configuration procedure.
* The RcfFileGenerator for MetroCluster IP also provides a per-port cabling overview for each switch. Use this cabling overview to verify your cabling.

Cabling eight-node MetroCluster configurations

For MetroCluster configuration running ONTAP 9.8 and earlier, some procedures that are performed to transition an upgrade require the addition of a second four-node DR group to the configuration to create a temporary eight-node configuration. Starting with ONTAP 9.9.1, permanent 8-node MetroCluster configurations are supported.

About this task

For such configurations, you use the same method as described above. Instead of a second MetroCluster, you are cabling an additional four-node DR group.

For example, your configuration includes the following:

* Cisco 3132Q-V switches
* MetroCluster 1: FAS2750 platforms
* MetroCluster 2: AFF A700 platforms (these platforms are being added as a second four-node DR group)

Steps

1. For MetroCluster 1, cable the Cisco 3132Q-V switches using the table for the FAS2750 platform and the rows for MetroCluster 1 interfaces.
2. For MetroCluster 2 (the second DR group), cable the Cisco 3132Q-V switches using the table for the AFF A700 platform and the rows for MetroCluster 2 interfaces.

Platform port assignments for Cisco 3132Q-V switches

The port usage in a MetroCluster IP configuration depends on the switch model and platform type.

Port usage for FAS2750 or AFF A220 systems and a Cisco 3132Q-V switch

Cabling an AFF A220 or FAS2750 to a Cisco 3132Q-V switch			
Port use	FAS2750. AFF A220		Switch Port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1
			2
			3
			4
			5
			6
ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	9/1
	disabled		9/2-4
	e0a	e0b	10/1
	disabled		10/2-4
MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	11/1
	disabled		11/2-4
	e0a	e0b	12/1
	disabled		12/2-4
MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	13/1
	disabled		13/2-4
	e0a	e0b	14/1
	disabled		14/2-4
ISL, MetroCluster native speed 40G	ISL, MetroCluster		15 - 20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Port usage for FAS9000, AFF A700 and a Cisco 3132Q-V switch

Cabling an AFF A700 or FAS9000 to a Cisco 3132Q-V switch			
Port use	**FAS9000, AFF A700**		**Switch port**
	IP_switch_x_1	**IP_switch_x_2**	**Port**
MetroCluster 1 Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2 Local Cluster interface			3
			4
MetroCluster 3 Local Cluster interface			5
			6
ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster		7
			8
MetroCluster 1 MetroCluster interface	e5a	e5b	9
	e5a	e5b	10
MetroCluster 2 MetroCluster interface	e5a	e5b	11
	e5a	e5b	12
MetroCluster 3 MetroCluster interface	e5a	e5b	13
	e5a	e5b	14
ISL, MetroCluster native speed 40G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Port usage for AFF A800 and a Cisco 3132Q-V switch

Cabling an AFF A800 to a Cisco 3132Q-V switch			
Port use	**AFF A800**		**Switch Port**
	IP_switch_x_1	**IP_switch_x_2**	
MetroCluster 1 Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2 Local Cluster interface			3
			4
MetroCluster 3 Local Cluster interface			5
			6
ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster		7
			8
MetroCluster 1 MetroCluster interface	e0b	e1b	9
	e0b	e1b	10
MetroCluster 2 MetroCluster interface	e0b	e1b	11
	e0b	e1b	12
MetroCluster 3 MetroCluster interface	e0b	e1b	13
	e0b	e1b	14
ISL, MetroCluster native speed 40G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Platform port assignments for Cisco 3232C or Cisco 9336C switches

The port usage in a MetroCluster IP configuration depends on the switch model and platform type.

Review these considerations before using the tables:

- The following tables show the port usage for site A. The same cabling is used for site B.
- The switches cannot be configured with ports of different speeds (for example, a mix of 100 Gbps ports and 40 Gbps ports).
- If you are configuring a single MetroCluster with the switches, use the **MetroCluster 1** port group.

  Keep track of the MetroCluster port group (MetroCluster 1, MetroCluster 2, or MetroCluster 3). You will need it when using the RcfFileGenerator tool as described later in this configuration procedure.

- The RcfFileGenerator for MetroCluster IP also provides a per-port cabling overview for each switch.

  Use this cabling overview to verify your cabling.

Cabling two MetroCluster configurations to the switches

When cabling more than one MetroCluster configuration to a Cisco 3132Q-V switch, then cable each MetroCluster according to the appropriate table. For example, if cabling a FAS2750 and an A700 to the same Cisco 3132Q-V switch. Then you cable the FAS2750 as per 'MetroCluster 1' in Table 1, and the A700 as per 'MetroCluster 2' or 'MetroCluster 3' in Table 2. You cannot physically cable both the FAS2750 and A700 as 'MetroCluster 1'.

Cabling a FAS2750 or AFF A220 system to a Cisco 3232C or Cisco 9336C switch

Cabling an AFF A220 or FAS2750 to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS2750, AFF A220		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1 - 6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	9/1
	disabled		9/2-4
	e0a	e0b	10/1
	disabled		10/2-4
MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	11/1
	disabled		11/2-4
	e0a	e0b	12/1
	disabled		12/2-4
MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	13/1
	disabled		13/2-4
	e0a	e0b	14/1
	disabled		14/2-4
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25 - 32

Cabling a AFF A300 or FAS8200 to a Cisco 3232C or Cisco 9336C switch

Cabling a AFF A300 or FAS8200 to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS8200, AFF A300		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1 Local Cluster interface	See Hardware Universe for available ports		1/1
			1/2 - 4
			2/1
			2/2 - 4
MetroCluster 2 Local Cluster interface			3/1
			3/2 - 4
			4/1
			4/2 - 4
MetroCluster 3 Local Cluster interface			5/1
			5/2 - 4
			6/1
			6/2 - 4
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1 MetroCluster interface	e1a	e1b	9/1
	disabled		9/2-4
	e1a	e1b	10/1
	disabled		10/2-4
MetroCluster 2 MetroCluster interface	e1a	e1b	11/1
	disabled		11/2-4
	e1a	e1b	12/1
	disabled		12/2-4
MetroCluster 3 MetroCluster interface	e1a	e1b	13/1
	disabled		13/2-4
	e1a	e1b	14/1
	disabled		14/2-4
ISL, MetroCluster	ISL, MetroCluster		15 - 20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
MetroCluster 4 MetroCluster interface	e1a	e1b	25/1
	disabled		25/2-4
	e1a	e1b	26/1
	disabled		26/2-4
Unused	-		27 - 28
MetroCluster 4 Local Cluster interface	See Hardware Universe		29/1
	disabled		29/2-4
	See Hardware Universe		30/1
	disabled		30/2-4
Unused	-		31 - 32

Cabling a AFF A250 or FAS500f to a Cisco 3232C or Cisco 9336C switch

<table>
<tr><th colspan="4">Cabling an AFF A250 or FAS500f to a Cisco 3232C or Cisco 9336C switch</th></tr>
<tr><th rowspan="2">Port use</th><th colspan="2">FAS500f, AFF A250</th><th rowspan="2">Switch port</th></tr>
<tr><th>IP_switch_x_1</th><th>IP_switch_x_2</th></tr>
<tr><td>Unused</td><td colspan="2">-</td><td>1 - 6</td></tr>
<tr><td rowspan="2">ISL, Local Cluster native speed / 100G</td><td colspan="2" rowspan="2">ISL, Local Cluster</td><td>7</td></tr>
<tr><td>8</td></tr>
<tr><td rowspan="4">MetroCluster 1, Shared Cluster and MetroCluster interface</td><td>e0c</td><td>e0d</td><td>9/1</td></tr>
<tr><td colspan="2">disabled</td><td>9/2-4</td></tr>
<tr><td>e0c</td><td>e0d</td><td>10/1</td></tr>
<tr><td colspan="2">disabled</td><td>10/2-4</td></tr>
<tr><td rowspan="4">MetroCluster 2, Shared Cluster and MetroCluster interface</td><td>e0c</td><td>e0d</td><td>11/1</td></tr>
<tr><td colspan="2">disabled</td><td>11/2-4</td></tr>
<tr><td>e0c</td><td>e0d</td><td>12/1</td></tr>
<tr><td colspan="2">disabled</td><td>12/2-4</td></tr>
<tr><td rowspan="4">MetroCluster 3, Shared Cluster and MetroCluster interface</td><td>e0c</td><td>e0d</td><td>13/1</td></tr>
<tr><td colspan="2">disabled</td><td>13/2-4</td></tr>
<tr><td>e0c</td><td>e0d</td><td>14/1</td></tr>
<tr><td colspan="2">disabled</td><td>14/2-4</td></tr>
<tr><td rowspan="6">ISL, MetroCluster native speed 40G / 100G</td><td colspan="2" rowspan="6">ISL, MetroCluster</td><td>15</td></tr>
<tr><td>16</td></tr>
<tr><td>17</td></tr>
<tr><td>18</td></tr>
<tr><td>19</td></tr>
<tr><td>20</td></tr>
<tr><td rowspan="4">ISL, MetroCluster breakout mode 10G</td><td colspan="2" rowspan="4">ISL, MetroCluster</td><td>21/1-4</td></tr>
<tr><td>22/1-4</td></tr>
<tr><td>23/1-4</td></tr>
<tr><td>24/1-4</td></tr>
<tr><td>Unused</td><td colspan="2">-</td><td>25 - 32</td></tr>
</table>

Cabling a AFF A320 to a Cisco 3232C or Cisco 9336C switch

Cabling a AFF A320 to a Cisco 3232C or Cisco 9336C switch			
Port use	**AFF A320**		**Switch port**
	IP_switch_x_1	**IP_switch_x_2**	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 3, Local Cluster interface			5
			6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	e0g	e0h	9
	e0g	e0h	10
MetroCluster 2, MetroCluster interface	e0g	e0h	11
	e0g	e0h	12
MetroCluster 3, MetroCluster interface	e0g	e0h	13
	e0g	e0h	14
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25
			26
			27
			28
			29
			30
			31
			32

Cabling an AFF A400, FAS8300 or FAS8700 to a Cisco 3232C or Cisco 9336C switch

Cabling a AFF A400, FAS8300 or FAS8700 to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS8300, FAS8700, AFF A400		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 3, Local Cluster interface			5
			6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	e1a	e1b	9
	e1a	e1b	10
MetroCluster 2, MetroCluster interface	e1a	e1b	11
	e1a	e1b	12
MetroCluster 3, MetroCluster interface	e1a	e1b	13
	e1a	e1b	14
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25
			26
			27
			28
			29
			30
			31
			32

Cabling a AFF A700 or FAS9000 to a Cisco 3232C or Cisco 9336C switch

Cabling a AFF A700 or FAS9000 to a Cisco 3232C or Cisco 9336C switch			
Port use	FAS9000, AFF A700		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 3, Local Cluster interface			5
			6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	e5a	e5b	9
	e5a	e5b	10
MetroCluster 2, MetroCluster interface	e5a	e5b	11
	e5a	e5b	12
MetroCluster 3, MetroCluster interface	e5a	e5b	13
	e5a	e5b	14
ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		15
			16
			17
			18
			19
			20
ISL, MetroCluster breakout mode 10G	ISL, MetroCluster		21/1-4
			22/1-4
			23/1-4
			24/1-4
Unused	-		25
			26
			27
			28
			29
			30
			31
			32

Cabling a AFF A800 to a Cisco 3232C or Cisco 9336C switch

<table>
<tr><th colspan="4">Cabling an AFF A800 to a Cisco 3232C or Cisco 9336C switch</th></tr>
<tr><th rowspan="2">Port use</th><th colspan="2">AFF A800</th><th rowspan="2">Switch port</th></tr>
<tr><th>IP_switch_x_1</th><th>IP_switch_x_2</th></tr>
<tr><td rowspan="2">MetroCluster 1,
Local Cluster interface</td><td colspan="2" rowspan="6">See Hardware Universe
for available ports</td><td>1</td></tr>
<tr><td>2</td></tr>
<tr><td rowspan="2">MetroCluster 2,
Local Cluster interface</td><td>3</td></tr>
<tr><td>4</td></tr>
<tr><td rowspan="2">MetroCluster 3,
Local Cluster interface</td><td>5</td></tr>
<tr><td>6</td></tr>
<tr><td rowspan="2">ISL, Local Cluster
native speed / 100G</td><td colspan="2" rowspan="2">ISL, Local Cluster</td><td>7</td></tr>
<tr><td>8</td></tr>
<tr><td rowspan="2">MetroCluster 1,
MetroCluster interface</td><td>e0b</td><td>e1b</td><td>9</td></tr>
<tr><td>e0b</td><td>e1b</td><td>10</td></tr>
<tr><td rowspan="2">MetroCluster 2,
MetroCluster interface</td><td>e0b</td><td>e1b</td><td>11</td></tr>
<tr><td>e0b</td><td>e1b</td><td>12</td></tr>
<tr><td rowspan="2">MetroCluster 3,
MetroCluster interface</td><td>e0b</td><td>e1b</td><td>13</td></tr>
<tr><td>e0b</td><td>e1b</td><td>14</td></tr>
<tr><td rowspan="6">ISL, MetroCluster
native speed
40G / 100G</td><td colspan="2" rowspan="6">ISL, MetroCluster</td><td>15</td></tr>
<tr><td>16</td></tr>
<tr><td>17</td></tr>
<tr><td>18</td></tr>
<tr><td>19</td></tr>
<tr><td>20</td></tr>
<tr><td rowspan="4">ISL, MetroCluster
breakout mode
10G</td><td colspan="2" rowspan="4">ISL, MetroCluster</td><td>21/1-4</td></tr>
<tr><td>22/1-4</td></tr>
<tr><td>23/1-4</td></tr>
<tr><td>24/1-4</td></tr>
<tr><td rowspan="8">Unused</td><td colspan="2" rowspan="8">-</td><td>25</td></tr>
<tr><td>26</td></tr>
<tr><td>27</td></tr>
<tr><td>28</td></tr>
<tr><td>29</td></tr>
<tr><td>30</td></tr>
<tr><td>31</td></tr>
<tr><td>32</td></tr>
</table>

Cabling an AFF A320, AFF A400, AFF A700 or AFF A800 to a Cisco 9336C-FX2 shared switch

Cabling an AFF A320, A400, A700, and A800 to a Cisco 9336C-FX2 shared switch			
MetroCluster 1, Local Cluster Interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster Interface			3
			4
Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b	5
	NSM-B, e0a	NSM-B, e0b	6
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		7
			8
MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'	9
	Port 'A'	Port 'B'	10
MetroCluster 2, MetroCluster interface	Port 'A'	Port 'B'	11
	Port 'A'	Port 'B'	12
ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	ISL, MetroCluster	ISL, MetroCluster	13
			14
			15
			16
MetroCluster 1, Storage Interface	See Hardware Universe for available ports		17
			18
MetroCluster 2, Storage Interface			19
			20
Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b	21
	NSM-B, e0a	NSM-B, e0b	22
Storage shelf 3 (7)	NSM-A, e0a	NSM-A, e0b	23
	NSM-B, e0a	NSM-B, e0b	24
Storage shelf 4 (6)	NSM-A, e0a	NSM-A, e0b	25
	NSM-B, e0a	NSM-B, e0b	26
Storage shelf 5 (5)	NSM-A, e0a	NSM-A, e0b	27
	NSM-B, e0a	NSM-B, e0b	28
Storage shelf 6 (4)	NSM-A, e0a	NSM-A, e0b	29
	NSM-B, e0a	NSM-B, e0b	30
Storage shelf 7 (3)	NSM-A, e0a	NSM-A, e0b	31
	NSM-B, e0a	NSM-B, e0b	32
Storage shelf 8 (2)	NSM-A, e0a	NSM-A, e0b	33
	NSM-B, e0a	NSM-B, e0b	34
Storage shelf 9 (1)	NSM-A, e0a	NSM-A, e0b	35
	NSM-B, e0a	NSM-B, e0b	36

MetroCluster interfaces per platform		
Platform	**Port 'A'**	**Port 'B'**
AFF A320	e0g	e0h
AFF A400	e1a	e1b
AFF A700	e5a	e5b
AFF A800	e0b	e1b

Platform port assignments for Broadcom supported BES-53248 IP switches

The port usage in a MetroCluster IP configuration depends on the switch model and platform type.

The switches cannot be configured with ports of different speeds (for example, a mix of 25 Gbps ports and 10 Gbps ports).

Notes for the tables below:

1. For some platforms, you can use ports 49 - 54 for MetroCluster ISLs or MetroCluster interface connections.

   These ports require an additional license.

2. Only a single AFF A320 system can be connected to the switch and no other platform can be connected at the same time.

   Features that require a switched cluster are not supported in this configuration, including MetroCluster FC to IP transition and tech refresh procedures.

3. AFF A320 systems configured with Broadcom BES-53248 switches might not support all features.

   Any configuration or feature that requires that the local cluster connections are connected to a switch is not supported. For example, the following configurations and procedures are not supported:

   - Eight-node MetroCluster configurations
   - Transitioning from MetroCluster FC to MetroCluster IP configurations
   - Refreshing a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Switch port usage for AFF A220 or FAS2750 systems

Cabling a AFF A220 or FAS2750 to a Broadcom BES-53248 switch			
Port use	FAS2750, A220		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1-6
MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	9
	e0a	e0b	10
MetroCluster 4, Shared Cluster and MetroCluster interface	e0a	e0b	11
	e0a	e0b	12
ISL, MetroCLuster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Unused	-		17 - 52
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		55
			56

Switch port usage for AFF A250 or FAS500f systems

Cabling a AFF A250 or FAS500f to a Broadcom BES-53248 switch			
Port use	FAS500f, A250		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1-6
MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	9
	e0c	e0d	10
MetroCluster 4, Shared Cluster and MetroCluster interface	e0c	e0d	11
	e0c	e0d	12
ISL, MetroCLuster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Unused	-		17 - 52
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		55
			56

Switch port usage for AFF A300 or FAS8200 systems

Cabling a AFF A300 or FAS8200 to a Broadcom BES-53248 switch			
Port use	FAS8200, AFF A300		Switch port
	IP_switch_x_1	IP_switch_x_2	
MetroCluster 1, Local Cluster interface	See Hardware Universe for available ports		1
			2
MetroCluster 2, Local Cluster interface			3
			4
MetroCluster 1, MetroCluster interface	e1a	e1b	5
	e1a	e1b	6
MetroCluster 2, MetroCluster interface	e1a	e1b	7
	e1a	e1b	8
Unused	-		9
			10
			11
			12
ISL, MetroCLuster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Unused	-		17 - 52
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		55
			56

Cabling a AFF A320 to a Broadcom BES-53248 switch			
Port use	AFF A320		Switch port
	IP_switch_x_1	IP_switch_x_2	
Ports not used	Ports not used		1 - 12
ISL, MetroCLuster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Ports not licensed (17 - 52)			..
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
MetroCluster 1, MetroCluster interface (see note 2)	e0g	e0h	55
	e0g	e0h	56

Switch port usage for AFF A400, FAS8300 or FAS8700 systems

Cabling a FAS8300, A400 or FAS8700 to a Broadcom BES-53248 switch

Port use	FAS8300,FAS8700, A400		Switch port
	IP_switch_x_1	IP_switch_x_2	
Unused	-		1 - 12
ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		13
			14
			15
			16
Unused	-		17 - 48
MetroCluster 5, Local Cluster interface (see note 1)	See Hardware Universe for available ports		49
			50
MetroCluster 5, MetroCluster interface (see note 1)	e1a	e1b	51
	e1a	e1b	52
ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster		53
			54
ISL, Local Cluster native speed / 100G	ISL, Local Cluster		55
			56

Cabling the controller peering, data, and management ports

You must cable the controller module ports used for cluster peering, management and data connectivity.

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.

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

2. Cable the controller’s management and data ports to the management and data networks at the local site.

   Use the installation instructions for your platform at the AFF and FAS System Documentation Center.

Configuring the IP switches

You must configure the switches for use as the cluster interconnect and for backend MetroCluster IP connectivity.

Configuring Broadcom IP switches

You must configure the Broadcom IP switches for use as the cluster interconnect and for backend MetroCluster IP connectivity.

Resetting the Broadcom IP switch to factory defaults

Before installing a new switch software version and RCFs, you must erase the Broadcom switch settings and perform basic configuration.

About this task

- You must repeat these steps on each of the IP switches in the MetroCluster IP configuration.
- You must be connected to the switch using the serial console.
- This task resets the configuration of the management network.

Steps

1. Change to the elevated command prompt (`#`): `enable`

   ```
   (IP_switch_A_1)> enable
   (IP_switch_A_1) #
   ```

2. Erase the startup configuration and remove the banner
   a. Erase the startup configuration:

      `erase startup-config`

      ```
      (IP_switch_A_1) #erase startup-config

      Are you sure you want to clear the configuration? (y/n) y

      (IP_switch_A_1) #
      ```

      This command does not erase the banner.

   b. Remove the banner:

      `no set clibanner`

      ```
      (IP_switch_A_1) # no set clibanner
      (IP_switch_A_1) #
      ```

3. Reboot the switch: **`(IP_switch_A_1) #reload`**

   ```
   Are you sure you would like to reset the system? (y/n) y
   ```

> If the system asks whether to save the unsaved or changed configuration before reloading the switch, select **No**.

4. Wait for the switch to reload, and then log in to the switch.

   The default user is “admin”, and no password is set. A prompt similar to the following is displayed:

   ```
   (Routing)>
   ```

5. Change to the elevated command prompt:

   `enable`

   ```
   Routing)> enable
   (Routing) #
   ```

6. Set the service port protocol to `none`:

   `serviceport protocol none`

   ```
   (Routing) #serviceport protocol none
   Changing protocol mode will reset ip configuration.
   Are you sure you want to continue? (y/n) y

   (Routing) #
   ```

7. Assign the IP address to the service port:

   `serviceport ip` *`ip-address netmask gateway`*

   The following example shows a service port assigned IP address "10.10.10.10" with subnet "255.255.255.0" and gateway "10.10.10.1":

   ```
   (Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
   ```

8. Verify that the service port is correctly configured:

   `show serviceport`

   The following example shows that the port is up and the correct addresses have been assigned:

```
(Routing) #show serviceport

Interface Status............................... Up
IP Address..................................... 10.10.10.10
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.10.10.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router............................ fe80::222:bdff:fef8:19ff
Configured IPv4 Protocol....................... None
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... D8:C4:97:56:87:D7

(Routing) #
```

9. If desired, configure the SSH server.

   The RCF file disables the Telnet protocol. If you do not configure the SSH server, you can only access the bridge using the serial port connection.

   a. Generate RSA keys.

   ```
   (Routing) #configure
   (Routing) (Config)#crypto key generate rsa
   ```

   b. Generate DSA keys (optional)

   ```
   (Routing) #configure
   (Routing) (Config)#crypto key generate dsa
   ```

   c. If you are using the FIPS compliant version of EFOS, generate the ECDSA keys. The following example creates the keys with a length of 256. Valid values are 256, 384 or 521.

   ```
   (Routing) #configure
   (Routing) (Config)#crypto key generate ecdsa 256
   ```

   d. Enable the SSH server.

   If necessary, exit the configuration context.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

> If keys already exist, then you might be asked to overwrite them.

10. If desired, configure the domain and name server:

    `configure`

    The following example shows the `ip domain` and `ip name server` commands:

```
(Routing) # configure
(Routing) (Config)#ip domain name lab.netapp.com
(Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
(Routing) (Config)#exit
(Routing) (Config)#
```

11. If desired, configure the time zone and time synchronization (SNTP).

    The following example shows the `sntp` commands, specifying the IP address of the SNTP server and the relative time zone.

```
(Routing) #
(Routing) (Config)#sntp client mode unicast
(Routing) (Config)#sntp server 10.99.99.5
(Routing) (Config)#clock timezone -7
(Routing) (Config)#exit
(Routing) (Config)#
```

12. Configure the switch name:

    `hostname IP_switch_A_1`

    The switch prompt will display the new name:

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. Save the configuration:

    `write memory`

    You receive prompts and output similar to the following example:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

14. Repeat the previous steps on the other three switches in the MetroCluster IP configuration.

Downloading and installing the Broadcom switch EFOS software

You must download the switch operating system file and RCF file to each switch in the MetroCluster IP configuration.

About this task

This task must be repeated on each switch in the MetroCluster IP configuration.

Note the following:

- When upgrading from EFOS 3.4.x.x to EFOS 3.7.x.x, the switch must be running EFOS 3.4.4.6 (or later 3.4.x.x release). If you are running a release prior to that, then upgrade the switch to EFOS 3.4.4.6 (or later 3.4.x.x release) first, then upgrade the switch to EFOS 3.7.x.x.
- The configuration for EFOS 3.4.x.x and 3.7.x.x are different. Changing the EFOS version from 3.4.x.x to 3.7.x.x or vice versa requires the switch to be reset to factory defaults and the RCF files for the corresponding EFOS version to be (re)applied. This procedure requires access through the serial console port.
- Starting with EFOS version 3.7.x.x, a non-FIPS compliant and a FIPS compliant version is available. Different steps apply when moving to from a non-FIPS compliant to a FIPS compliant version or vice versa. Changing EFOS from a non-FIPS compliant to a FIPS compliant version or vice versa will reset the switch to factory defaults. This procedure requires access through the serial console port.

Procedure	Current EFOS version	New EFOS version	High level steps
Steps to upgrade EFOS between two (non) FIPS compliant versions	3.4.x.x	3.4.x.x	Install the new EFOS image using method 1) The configuration and license information is retained
	3.4.4.6 (or later 3.4.x.x)	3.7.x.x non-FIPS compliant	Upgrade EFOS using method 1. Reset the switch to factory defaults and apply the RCF file for EFOS 3.7.x.x
	3.7.x.x non-FIPS compliant	3.4.4.6 (or later 3.4.x.x)	Downgrade EFOS using method 1. Reset the switch to factory defaults and apply the RCF file for EFOS 3.4.x.x
		3.7.x.x non-FIPS compliant	Install the new EFOS image using method 1. The configuration and license information is retained
	3.7.x.x FIPS compliant	3.7.x.x FIPS compliant	Install the new EFOS image using method 1. The configuration and license information is retained
Steps to upgrade to/from a FIPS compliant EFOS version	Non-FIPS compliant	FIPS compliant	Installation of the EFOS image using method 2. The switch configuration and license information will be lost.
	FIPS compliant	Non-FIPS compliant	

- Method 1: Steps to upgrade EFOS with downloading the software image to the backup boot partition
- Method 2: Steps to upgrade EFOS using the ONIE OS installation

Steps to upgrade EFOS with downloading the software image to the backup boot partition

You can perform the following steps only if both EFOS versions are non-FIPS compliant or both EFOS versions are FIPS compliant.

> Do not use these steps if one version is FIPS compliant and the other version is non-FIPS compliant.

Steps

1. Copy the switch software to the switch: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   In this example, the efos-3.4.4.6.stk operating system file is copied from the SFTP server at 50.50.50.50 to the backup partition. You need to use the IP address of your TFTP/SFTP server and the file name of the

RCF file that you need to install.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*************

Mode........................................... SFTP
Set Server IP.................................. 50.50.50.50
Path........................................... /switchsoftware/
Filename....................................... efos-3.4.4.6.stk
Data Type...................................... Code
Destination Filename........................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Set the switch to boot from the backup partition on the next switch reboot:

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Verify that the new boot image will be active on the next boot:

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Save the configuration:

`write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Reboot the switch:

`reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

6. Wait for the switch to reboot.

In rare scenarios the switch may fail to boot. Follow the Steps to upgrade EFOS using the ONIE OS installation to install the new image.

7. If you change the switch from EFOS 3.4.x.x to EFOS 3.7.x.x or vice versa then follow the following two procedures to apply the correct configuration (RCF):
   a. Resetting the Broadcom IP switch to factory defaults
   b. Downloading and installing the Broadcom RCF files
8. Repeat these steps on the remaining three IP switches in the MetroCluster IP configuration.

Steps to upgrade EFOS using the ONIE OS installation

You can perform the following steps if one EFOS version is FIPS compliant and the other EFOS version is non-FIPS compliant. These steps can be used to install the non-FIPS or FIPS compliant EFOS 3.7.x.x image from ONIE if the switch fails to boot.

Steps

1. Boot the switch into ONIE installation mode.

   During boot, select ONIE when the following screen appears:

```
+--------------------------------------------------------------------+
|EFOS                                                                |
|*ONIE                                                               |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
+--------------------------------------------------------------------+
```

   After selecting "ONIE", the switch will then load and present you with the following choices:

```
+--------------------------------------------------------------------+
|*ONIE: Install OS                                                   |
| ONIE: Rescue                                                       |
| ONIE: Uninstall OS                                                 |
| ONIE: Update ONIE                                                  |
| ONIE: Embed ONIE                                                   |
| DIAG: Diagnostic Mode                                              |
| DIAG: Burn-In Mode                                                 |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
+--------------------------------------------------------------------+
```

The switch now will boot into ONIE installation mode.

2. Stop the ONIE discovery and configure the ethernet interface

   Once the following message appears press <enter> to invoke the ONIE console:

```
 Please press Enter to activate this console. Info: eth0:  Checking
link... up.
 ONIE:/ #
```

   The ONIE discovery will continue and messages will be printed to the console.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Configure the ethernet interface and add the route using `ifconfig eth0 <ipAddress> netmask <netmask> up` and `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Verify that the server hosting the ONIE installation file is reachable:

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Install the new switch software

```
ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer            100% |*******************************| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

The software will install and then reboot the switch. Let the switch reboot normally into the new EFOS version.

6. Verify that the new switch software is installed

show bootvar

```
(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active      backup   current-active  next-active
----    ----------- -------- --------------- ------------
1   3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #
```

7. Complete the installation

   The switch will reboot with no configuration applied and reset to factory defaults. Follow the two procedures to configure the switch basic settings and apply the RCF file as outlined in the following two documents:

   a. Configure the switch basic settings. Follow step 4 and later: Resetting the Broadcom IP switch to factory defaults

   b. Create and apply the RCF file as outlined in Downloading and installing the Broadcom RCF files

Downloading and installing the Broadcom RCF files

You must download and install the switch RCF file to each switch in the MetroCluster IP configuration.

Before you begin

This task requires file transfer software, such as FTP, TFTP, SFTP, or SCP, to copy the files to the switches.

About this task

These steps must be repeated on each of the IP switches in the MetroCluster IP configuration.

There are four RCF files, one for each of the four switches in the MetroCluster IP configuration. You must use the correct RCF files for the switch model you are using.

Switch	RCF file
IP_switch_A_1	v1.32_Switch-A1.txt
IP_switch_A_2	v1.32_Switch-A2.txt
IP_switch_B_1	v1.32_Switch-B1.txt
IP_switch_B_2	v1.32_Switch-B2.txt

> The RCF files for EFOS version 3.4.4.6 or later 3.4.x.x. release and EFOS version 3.7.0.4 are different. You need to make sure that you have created the correct RCF files for the EFOS version that the switch is running.

EFOS version	RCF file version
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

Steps

1. Generate the Broadcom RCF files for MetroCluster IP.

   a. Download the RcfFileGenerator for MetroCluster IP

   b. Generate the RCF file for your configuration using the RcfFileGenerator for MetroCluster IP

2. Copy the RCF files to the switches:

   a. Copy the RCF files to the first switch: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF nvram:script BES-53248_v1.32_Switch-`

```
A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr
```

In this example, the "BES-53248_v1.32_Switch-A1.txt" RCF file is copied from the SFTP server at "50.50.50.50" to the local bootflash. You need to use the IP address of your TFTP/SFTP server and the file name of the RCF file that you need to install.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode........................................... SFTP
Set Server IP.................................. 50.50.50.50
Path........................................... /RcfFiles/
Filename....................................... BES-
53248_v1.32_Switch-A1.txt
Data Type...................................... Config Script
Destination Filename........................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"*********************************************************************
*******

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248


...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Verify that the RCF file is saved as a script:

`script list`

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr            852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Apply the RCF script:

`script apply BES-53248_v1.32_Switch-A1.scr`

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"**********************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Save the configuration:

`write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Reboot the switch:

`reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

f. Repeat the previous steps for each of the other three switches, being sure to copy the matching RCF file to the corresponding switch.

3. Reload the switch:

   `reload`

   ```
   IP_switch_A_1# reload
   ```

4. Repeat the previous steps on the other three switches in the MetroCluster IP configuration.

Configure Cisco IP switches

Configuring Cisco IP switches

You must configure the Cisco IP switches for use as the cluster interconnect and for backend MetroCluster IP connectivity.

Resetting the Cisco IP switch to factory defaults

Before installing a new software version and RCFs, you must erase the Cisco switch configuration and perform basic configuration.

You must repeat these steps on each of the IP switches in the MetroCluster IP configuration.

1. Reset the switch to factory defaults:

a. Erase the existing configuration: `write erase`

b. Reload the switch software: `reload`

   The system reboots and enters the configuration wizard. During the boot, if you receive the prompt Abort Auto Provisioning and continue with normal setup?(yes/no)[n], you should respond `yes` to proceed.

c. In the configuration wizard, enter the basic switch settings:

   - Admin password
   - Switch name
   - Out-of-band management configuration
   - Default gateway
   - SSH service (RSA) After completing the configuration wizard, the switch reboots.

d. When prompted, enter the user name and password to log in to the switch.

   The following example shows the prompts and system responses when configuring the switch. The angle brackets (<<<) show where you enter the information.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
  Confirm the password for "admin": password
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

You enter basic information in the next set of prompts, including the switch name, management address, and gateway, and select SSH with RSA.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

The final set of prompts completes the configuration:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-
Plane is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Save the configuration:

```
IP_switch-A-1# copy running-config startup-config
```

3. Reboot the switch and wait for the switch to reload:

```
IP_switch-A-1# reload
```

4. Repeat the previous steps on the other three switches in the MetroCluster IP configuration.

Downloading and installing the Cisco switch NX-OS software

You must download the switch operating system file and RCF file to each switch in the MetroCluster IP configuration.

This task requires file transfer software, such as FTP, TFTP, SFTP, or SCP, to copy the files to the switches.

These steps must be repeated on each of the IP switches in the MetroCluster IP configuration.

You must use the supported switch software version.

NetApp Hardware Universe

1. Download the supported NX-OS software file.

   Cisco Software Download

2. Copy the switch software to the switch: `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

   In this example, the nxos.7.0.3.I4.6.bin file is copied from SFTP server 10.10.99.99 to the local bootflash:

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
```

3. Verify on each switch that the switch NX-OS files are present in each switch's bootflash directory: `dir bootflash:`

   The following example shows that the files are present on IP_switch_A_1:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Install the switch software: `install all nxos bootflash:nxos.version-number.bin`

   The switch will reload (reboot) automatically after the switch software has been installed.

   The following example shows the software installation on IP_switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
-- SUCCESS
```

```
Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Wait for the switch to reload and then log in to the switch.

   After the switch has rebooted the login prompt is displayed:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verify that the switch software has been installed: `show version`

   The following example shows the output:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Repeat these steps on the remaining three IP switches in the MetroCluster IP configuration.

Downloading and installing the Cisco IP RCF files

You must download the RCF file to each switch in the MetroCluster IP configuration.

This task requires file transfer software, such as FTP, TFTP, SFTP, or SCP, to copy the files to the switches.

These steps must be repeated on each of the IP switches in the MetroCluster IP configuration.

You must use the supported switch software version.

NetApp Hardware Universe

There are four RCF files, one for each of the four switches in the MetroCluster IP configuration. You must use the correct RCF files for the switch model you are using.

Switch	RCF file
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_switch_B_2	NX3232_v1.80_Switch-B2.txt

Steps

1. Download the MetroCluster IP RCF files.
2. Copy the RCF files to the switches:
   a. Copy the RCF files to the first switch: `copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF bootflash: vrf management`

      In this example, the NX3232_v1.80_Switch-A1.txt RCF file is copied from the SFTP server at 10.10.99.99 to the local bootflash. You must use the IP address of your TFTP/SFTP server and the file name of the RCF file that you need to install.

      ```
      IP_switch_A_1# copy
      sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt
      bootflash: vrf management
      root@10.10.99.99's password: password
      sftp> progress
      Progress meter enabled
      sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
      /bootflash/NX3232_v1.80_Switch-A1.txt
      Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
      /bootflash/NX3232_v1.80_Switch-A1.txt
      /tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
      00:00
      sftp> exit
      Copy complete, now saving to disk (please wait)...
      IP_switch_A_1#
      ```

   b. Repeat the previous substep for each of the other three switches, being sure to copy the matching RCF file to the corresponding switch.

3. Verify on each switch that the RCF file is present in each switch's bootflash directory: `dir bootflash:`

   The following example shows that the files are present on IP_switch_A_1:

   ```
   IP_switch_A_1# dir bootflash:
                     .
                     .
                     .
   5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                     .
                     .
                     .

   Usage for bootflash://sup-local
   1779363840 bytes used
   13238841344 bytes free
   15018205184 bytes total
   IP_switch_A_1#
   ```

4. Configure the TCAM regions on Cisco 3132Q-V and Cisco 3232C switches.

   Skip this step if you do not have Cisco 3132Q-V or Cisco 3232C switches.

   a. On Cisco 3132Q-V switch, set the following TCAM regions:

   ```
   conf t
   hardware access-list tcam region span 0
   hardware access-list tcam region racl 256
   hardware access-list tcam region e-racl 256
   hardware access-list tcam region qos 256
   ```

   b. On Cisco 3232C switch, set the following TCAM regions:

   ```
   conf t
   hardware access-list tcam region span 0
   hardware access-list tcam region racl-lite 0
   hardware access-list tcam region racl 256
   hardware access-list tcam region e-racl 256
   hardware access-list tcam region qos 256
   ```

   c. After setting the TCAM regions, save the configuration and reload the switch:

```
copy running-config startup-config
reload
```

5. Copy the matching RCF file from the local bootflash to the running configuration on each switch: `copy bootflash:switch-specific-RCF.txt running-config`
6. Copy the RCF files from the running configuration to the startup configuration on each switch: `copy running-config startup-config`

   You should see output similar to the following:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Reload the switch: `reload`

```
IP_switch_A_1# reload
```

8. Repeat the previous steps on the other three switches in the MetroCluster IP configuration.

Configuring MACsec encryption on Cisco 9336C switches

You must only configure MACsec encryption on the WAN ISL ports that run between the sites. You must configure MACsec after applying the correct RCF file.

Licensing requirements for MACsec

MACsec requires a security license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply for licenses, see the Cisco NX-OS Licensing Guide

Enabling Cisco MACsec Encryption WAN ISLs in MetroCluster IP configurations

You can enable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

1. Enter the global configuration mode: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Enable MACsec and MKA on the device: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Copy the running configuration to the startup configuration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Disabling Cisco MACsec Encryption WAN ISLs in MetroCluster IP configurations

You might need to disable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

1. Enter the global configuration mode: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Disable the MACsec configuration on the device: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

> Selecting the no option restores the MACsec feature.

3. Select the interface that you already configured with MACsec.

   You can specify the interface type and identity. For an Ethernet port, use ethernet slot/port.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Remove the keychain, policy and fallback-keychain configured on the interface to remove the MACsec configuration: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

5. Repeat steps 3 and 4 on all interfaces where MACsec is configured.
6. Copy the running configuration to the startup configuration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Configuring a MACsec key chain and keys

You can create a MACsec key chain or keys on your configuration.

Key Lifetime and Hitless Key Rollover

A MACsec keychain can have multiple pre-shared keys (PSKs), each configured with a key ID and an optional lifetime. A key lifetime specifies at which time the key activates and expires. In the absence of a lifetime configuration, the default lifetime is unlimited. When a lifetime is configured, MKA rolls over to the next configured pre-shared key in the keychain after the lifetime is expired. The time zone of the key can be local or UTC. The default time zone is UTC. A key can roll over to a second key within the same keychain if you configure the second key (in the keychain) and configure a lifetime for the first key. When the lifetime of the first key expires, it automatically rolls over to the next key in the list. If the same key is configured on both sides of the link at the same time, then the key rollover is hitless (that is, the key rolls over without traffic interruption).

Fallback Key

A MACsec session can fail due to a key/key name (CKN) mismatch or a finite key duration between the switch and a peer. If a MACsec session does fail, a fallback session can take over if a fallback key is configured. A fallback session prevents downtime due to primary session failure and allows a user time to fix the key issue causing the failure. A fallback key also provides a backup session if the primary session fails to start. This feature is optional.

1. Enter the global configuration mode: `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. To hide the encrypted key octet string, replace the string with a wildcard character in the output of the show running-config and show startup-config commands:

   ```
   IP_switch_A_1(config)# key-chain macsec-psk no-show
   ```

   NOTE:

   The octet string is also hidden when you save the configuration to a file.

   By default, PSK keys are displayed in encrypted format and can easily be decrypted. This command applies only to MACsec key chains.

3. Create a MACsec key chain to hold a set of MACsec keys and enter MACsec key chain configuration mode: `key chain name macsec`

   ```
   IP_switch_A_1(config)# key chain 1 macsec
   IP_switch_A_1(config-macseckeychain)#
   ```

4. Create a MACsec key and enter MACsec key configuration mode: `key key-id`

   The range is from 1 to 32 hex digit key-string, and the maximum size is 64 characters.

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

5. Configure the octet string for the key: `key-octet-string octet-string cryptographic-algorithm AES_128_CMAC | AES_256_CMAC`

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
cryptographic-algorithm AES_256_CMAC
```

> The octet-string argument can contain up to 64 hexadecimal characters. The octet key is encoded internally, so the key in clear text does not appear in the output of theshow running-config macsec command.

6. Configure a send lifetime for the key (in seconds): `send-lifetime start-time duration duration`

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

By default, the device treats the start time as UTC. The start-time argument is the time of day and date that the key becomes active. The duration argument is the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).

7. Copy the running configuration to the startup configuration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

8. Displays the keychain configuration: `show keychain name`

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Configuring a MACsec policy

1. Enter the global configuration mode: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Create a MACsec policy: `macsec policy name`

```
IP_switch_A_1(config)# macsec policy abc
IP_switch_A_1(config-macsec-policy)#
```

3. Configure one of the following ciphers, GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, or GCM-AES-XPN-256: `cipher-suite name`

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Configure the key server priority to break the tie between peers during a key exchange: `key-server-priority number`

```
switch(config-macsec-policy)# key-server-priority 0
```

5. Configure the security policy to define the handling of data and control packets: `security-policy security policy`

   Choose a security policy from the following options:

   - must-secure — packets not carrying MACsec headers are dropped
   - should-secure — packets not carrying MACsec headers are permitted (this is the default value)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configure the replay protection window so the secured interface does not accept a packet that is less than the configured window size: `window-size number`

   > The replay protection window size represents the maximum out-of-sequence frames that MACsec accepts and are not discarded. The range is from 0 to 596000000.

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. Configure the time in seconds to force an SAK rekey: `sak-expiry-time time`

   You can use this command to change the session key to a predictable time interval. The default is 0.

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. Configure one of the following confidentiality offsets in the layer 2 frame where encryption begins: `conf-offsetconfidentiality offset`

   Choose from the following options:

- CONF-OFFSET-0.
- CONF-OFFSET-30.
- CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

+ NOTE: This command might be necessary for intermediate switches to use packet headers (dmac, smac, etype) like MPLS tags.

9. Copy the running configuration to the startup configuration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

10. Display the MACsec policy configuration: `show macsec policy`

```
IP_switch_A_1(config-macsec-policy)# show macsec policy
```

Verifying the MACsec configuration

1. Repeat **all** of the previous procedures on the second switch within the configuration to establish a MACsec session.
2. Run the following commands to verify that both switches are successfully encrypted:

   a. Run: `show macsec mka summary`

   b. Run: `show macsec mka session`

   c. Run: `show macsec mka statistics`

   You can verify the MACsec configuration using the following commands:

   +

Command	Displays information about…
`show macsec mka session interface typeslot/port number`	The MACsec MKA session for a specific interface or for all interfaces
`show key chain name`	The key chain configuration
`show macsec mka summary`	The MACsec MKA configuration
`show macsec policy policy-name`	The configuration for a specific MACsec policy or for all MACsec policies

Configuring a MACsec fallback key on a WAN ISL port

You can configure a fallback key to initiate a backup session if the primary session fails as a result of a key/key name (CKN) mismatch or a finite key duration between the switch and peer.

1. Enter the global configuration mode: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Specify the interface that you are configuring.

   You can specify the interface type and identity. For an Ethernet port, use `ethernet slot/port`

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

3. Specify the fallback key chain for use after a MACsec session failure due to a key/key ID mismatch or a key expiration: `macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

   > You should configure the fallback-keychain using the steps, *Configuring a MACsec key chain and keys* before proceeding with this step.

```
IP_switch_A_1(config-if)# macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

4. Repeat the previous steps to configure additional WAN ISL ports with MACsec.
5. Copy the running configuration to the startup configuration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Setting Forward Error Correction for systems using 25-Gbps connectivity

If your system is configured using 25-Gbps connectivity, you need to set the Forward Error Correction (fec) parameter manually to off after applying the RCF file. The RCF file does not apply this setting.

The 25-Gbps ports must be cabled prior to performing this procedure.

Platform port assignments for Cisco 3232C or Cisco 9336C switches

This task only applies to platforms using 25-Gbps connectivity: • AFF A300 • FAS 8200 • FAS 500f • AFF A250

This task must be performed on all four switches in the MetroCluster IP configuration.

1. Set the fec parameter to off on each 25-Gbps port that is connected to a controller module, and then copy the running configuration to the startup configuration:

   a. Enter configuration mode: `config t`

   b. Specify the 25-Gbps interface to configure: `interface interface-ID`

   c. Set fec to off: `fec off`

   d. Repeat the previous steps for each 25-Gbps port on the switch.

   e. Exit configuration mode: `exit`

   The following example shows the commands for interface Ethernet1/25/1 on switch IP_switch_A_1:

   +

   ```
   IP_switch_A_1# conf t
   IP_switch_A_1(config)# interface Ethernet1/25/1
   IP_switch_A_1(config-if)# fec off
   IP_switch_A_1(config-if)# exit
   IP_switch_A_1(config-if)# end
   IP_switch_A_1# copy running-config startup-config
   ```

2. Repeat the previous step on the other three switches in the MetroCluster IP configuration.

Configuring MACsec encryption on Cisco 9336C switches

If desired, you can configure MACsec encryption on the WAN ISL ports that run between the sites. You must configure MACsec after applying the correct RCF file.

ⓘ MACsec encryption can only be applied to the WAN ISL ports.

Licensing requirements for MACsec

MACsec requires a security license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply for licenses, see the Cisco NX-OS Licensing Guide

Enabling Cisco MACsec Encryption WAN ISLs in MetroCluster IP configurations

You can enable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

1. Enter the global configuration mode: `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Enable MACsec and MKA on the device: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Copy the running configuration to the startup configuration: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Disabling Cisco MACsec Encryption

You might need to disable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

> ⓘ If you disable encryption, you must also delete your keys, as described in XXX.

1. Enter the global configuration mode: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Disable the MACsec configuration on the device: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

> ⓘ Selecting the no option restores the MACsec feature.

3. Select the interface that you already configured with MACsec.

   You can specify the interface type and identity. For an Ethernet port, use ethernet slot/port.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Remove the keychain, policy and fallback-keychain configured on the interface to remove the MACsec configuration: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

5. Repeat steps 3 and 4 on all interfaces where MACsec is configured.
6. Copy the running configuration to the startup configuration: `copy running-config startup-config`

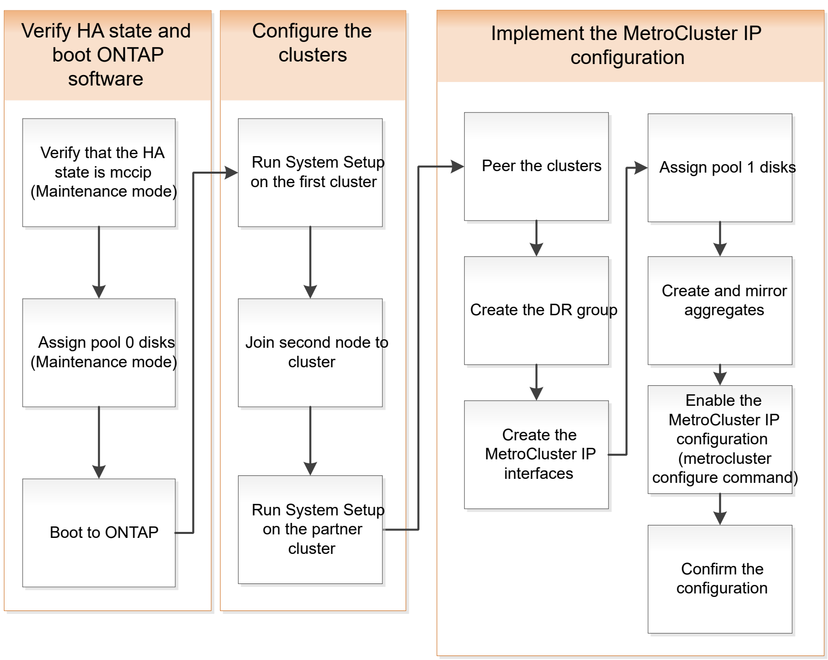
```
IP_switch_A_1(config)# copy running-config startup-config
```

Configuring a MACsec key chain and keys

For details on configuring a MACsec key chain, see the Cisco documentation for your switch.

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.



Handling eight-node Configurations

An eight-node configuration will consist of two DR groups. Configure the first DR group by using the tasks in this section.

Then perform the tasks in Expanding a four-node MetroCluster IP configuration to an eight-node configuration

Gathering required information

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

You can use these links to download csv files and fill in the tables with your site-specific information.

MetroCluster IP setup worksheet, site_A

MetroCluster IP setup worksheet, site_B

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.

Configuration step	Standard cluster configuration	MetroCluster configuration
Configure management, cluster, and data LIFs on each node.	Same in both types of clusters	Configure the root aggregate.
Same in both types of clusters	Set up the cluster on one node in the cluster.	Same in both types of clusters
Join the other node to the cluster.	Same in both types of clusters	Create a mirrored root aggregate.
Optional	Required	Peer the clusters.
Optional	Required	Enable the MetroCluster configuration.

Verifying the ha-config state of components

In a MetroCluster IP configuration that is not preconfigured at the factory, you must verify that the ha-config state of the controller and chassis components is set to "mccip" 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. Display the HA state of the controller module and chassis:

   ```
   ha-config show
   ```

   The controller module and chassis should show the value "mccip".

2. If the displayed system state of the controller is not "mccip", set the HA state for the controller:

```
ha-config modify controller mccip
```

3. If the displayed system state of the chassis is not "mccip", set the HA state for the chassis:

```
ha-config modify chassis mccip
```

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

Restoring system defaults on a controller module

Reset and restore defaults on the controller modules.

1. At the LOADER prompt, return environmental variables to their default setting: `set-defaults`
2. Boot the node to the boot menu: `boot_ontap menu`

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

3. Clear the node configuration:

   - If you are using systems configured for ADP, select option `9a` from the boot menu, and respond `yes` when prompted.

     > This process is disruptive.

     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)?  9a
########## WARNING ##########

    This is a disruptive operation and will result in the
    loss of all filesystem data. Before proceeding further,
    make sure that:
    1) This option (9a) has been executed or will be executed
    on the HA partner node, prior to reinitializing either
    system in the HA-pair.
    2) The HA partner node is currently in a halted state or
    at the LOADER prompt.


    Do you still want to continue (yes/no)? yes
```

- If your system is not configured for ADP, type `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.
```

Manually assigning drives to pool 0

If you did not receive the systems pre-configured from the factory, you might have to manually assign the pool 0 drives. Depending on the platform model and whether the system is using ADP, you must manually assign drives to pool 0 for each node in the MetroCluster IP configuration. The procedure you use depends on the version of ONTAP you are using.

- Manually assigning drives for pool 0 (ONTAP 9.4 and later)
- Manually assigning drives for pool 0 (ONTAP 9.3)

Manually assigning drives for pool 0 (ONTAP 9.4 and later)

If the system has not been pre-configured at the factory and does not meet the requirements for automatic drive assignment, you must manually assign the pool 0 drives.

About this task

This procedure applies to configurations running ONTAP 9.4 or later.

To determine if your system requires manual disk assignment, you should review Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later.

You perform these steps in Maintenance mode. The procedure must be performed on each node in the configuration.

Examples in this section are based on the following assumptions:

- node_A_1 and node_A_2 own drives on:
  - site_A-shelf_1 (local)
  - site_B-shelf_2 (remote)

- node_B_1 and node_B_2 own drives on:
  - site_B-shelf_1 (local)
  - site_A-shelf_2 (remote)

Steps

1. Display the boot menu:

   `boot_ontap menu`

2. Select option "9a".

   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)?  9a
   ########## WARNING ##########

       This is a disruptive operation and will result in the
       loss of all filesystem data. Before proceeding further,
       make sure that:
       1) This option (9a) has been executed or will be executed
       on the HA partner node (and DR/DR-AUX partner nodes if
       applicable), prior to reinitializing any system in the
       HA-pair (or MetroCluster setup).
       2) The HA partner node (and DR/DR-AUX partner nodes if
       applicable) is currently waiting at the boot menu.

       Do you still want to continue (yes/no)? yes
   ```

3. When the node restarts, press Ctrl-C when prompted to display the boot menu, and then select the option for **Maintenance mode boot**.
4. In Maintenance mode, manually assign drives for the local aggregates on the node:

   `disk assign *disk-id* -p 0 -s *local-node-sysid*`

   The drives should be assigned symmetrically, so each node has an equal number of drives. The following steps are for a configuration with two storage shelves at each site.

a. When configuring node_A_1, manually assign drives from slot 0 to 11 to pool0 of node A1 from site_A-shelf_1.
b. When configuring node_A_2, manually assign drives from slot 12 to 23 to pool0 of node A2 from site_A-shelf_1.
c. When configuring node_B_1, manually assign drives from slot 0 to 11 to pool0 of node B1 from site_B-shelf_1.
d. When configuring node_B_2, manually assign drives from slot 12 to 23 to pool0 of node B2 from site_B-shelf_1.

5. Exit Maintenance mode:

```
halt
```

6. Display the boot menu:

```
boot_ontap menu
```

7. Select option "4" from the boot menu and let the system boot.
8. Repeat these steps on the other nodes in the MetroCluster IP configuration.
9. Proceed to Setting up ONTAP.

Manually assigning drives for pool 0 (ONTAP 9.3)

If you have at least two disk shelves for each node, you use ONTAP's auto-assignment functionality to automatically assign the local (pool 0) disks.

About this task

While the node is in Maintenance mode, you must first assign a single disk on the appropriate shelves to pool 0. ONTAP then automatically assign the rest of the disks on the shelf to the same pool. This task is not required on systems received from the factory, which have pool 0 to contain the pre-configured root aggregate.

This procedure applies to configurations running ONTAP 9.3.

This procedure is not required if you received your MetroCluster configuration from the factory. Nodes from the factory are configured with pool 0 disks and root aggregates.

This procedure can be used only if you have at least two disk shelves for each node, which allows shelf-level autoassignment of disks. If you cannot use shelf-level autoassignment, you must manually assign your local disks so that each node has a local pool of disks (pool 0).

These steps must be performed in Maintenance mode.

Examples in this section assume the following disk shelves:

- node_A_1 owns disks on:
  - site_A-shelf_1 (local)
  - site_B-shelf_2 (remote)
- node_A_2 is connected to:
  - site_A-shelf_3 (local)
  - site_B-shelf_4 (remote)

- node_B_1 is connected to:
  - site_B-shelf_1 (local)
  - site_A-shelf_2 (remote)
- node_B_2 is connected to:
  - site_B-shelf_3 (local)
  - site_A-shelf_4 (remote)

Steps

1. Manually assign a single disk for root aggregate on each node:

   `disk assign` *`disk-id`* `-p 0 -s` *`local-node-sysid`*

   The manual assignment of these disks allows the ONTAP autoassignment feature to assign the rest of the disks on each shelf.

   a. On node_A_1, manually assign one disk from local site_A-shelf_1 to pool 0.

   b. On node_A_2, manually assign one disk from local site_A-shelf_3 to pool 0.

   c. On node_B_1, manually assign one disk from local site_B-shelf_1 to pool 0.

   d. On node_B_2, manually assign one disk from local site_B-shelf_3 to pool 0.

2. Boot each node at site A, using option "4" on the boot menu:

   You should complete this step on a node before proceeding to the next node.

   a. Exit Maintenance mode:

      ```
      halt
      ```

   b. Display the boot menu:

      ```
      boot_ontap menu
      ```

   c. Select option "4" from the boot menu and proceed.

3. Boot each node at site B, using option "4" on the boot menu:

   You should complete this step on a node before proceeding to the next node.

   a. Exit Maintenance mode:

      ```
      halt
      ```

   b. Display the boot menu:

      ```
      boot_ontap menu
      ```

   c. Select option "4" from the boot menu and proceed.

Setting up ONTAP

After you boot each node, you are prompted to perform basic node and cluster configuration. After configuring the cluster, you return to the ONTAP CLI to create aggregates and create the MetroCluster configuration.

Before you begin

- You must have cabled the MetroCluster configuration.
- You must not have configured the Service Processor.

If you need to netboot the new controllers, see Netbooting the new controller modules in the *MetroCluster Upgrade, Transition, and Expansion Guide*.

About this task

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

Steps

1. Power up each node at the local site if you have not already done so and let them all boot completely.

   If the system is in Maintenance mode, you need to issue the halt command to exit Maintenance mode, and then issue the `boot_ontap` command to boot the system and get to cluster setup.

2. On the first node in each cluster, proceed through the prompts to configure the cluster

   a. Enable the AutoSupport tool by following the directions provided by the system.

      The output should be similar to the following:

```
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.

    This system will send event messages and periodic 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}: yes

.
.
.
```

b. Configure the node management interface by responding to the prompts.

The prompts are similar to the following:

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.229
has been created.
```

c. Create the cluster by responding to the prompts.

The prompts are similar to the following:

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


Do you intend for this node to be used as a single node cluster?
{yes, no} [no]:
no

Existing cluster interface configuration found:

Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]: no

Enter the cluster administrator's (username "admin") password:

Retype the password:


Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.

List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A

Creating cluster cluster_A

Starting cluster support services ...

Cluster cluster_A has been created.
```

d. Add licenses, set up a Cluster Administration SVM, and enter DNS information by responding to the prompts.

   The prompts are similar to the following:

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:


Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.


Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

e. Enable storage failover and set up the node by responding to the prompts.

   The prompts are similar to the following:

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: site_A
```

f. Complete the configuration of the node, but do not create data aggregates.

   You can use ONTAP System Manager, pointing your web browser to the cluster management IP address (https://172.17.12.153).

   Cluster management using System Manager (Versions 9.0 to 9.6)

   ONTAP System Manager (Versions 9.7 and later)

3. Boot the next controller and join it to the cluster, following the prompts.
4. Confirm that nodes are configured in high-availability mode:

   `storage failover show -fields mode`

   If not, you must configure HA mode on each node, and then reboot the nodes:

   `storage failover modify -mode ha -node localhost`

   This command configures high-availability mode but does not enable storage failover. Storage failover is automatically enabled when you configure the MetroCluster configuration later in the process.

5. Confirm that you have four ports configured as cluster interconnects:

   `network port show`

   The MetroCluster IP interfaces are not configured at this time and do not appear in the command output.

   The following example shows two cluster ports on node_A_1:

```
cluster_A::*> network port show -role cluster



Node: node_A_1


Ignore
```

```
                                                  Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


Node: node_A_2


Ignore

                                                  Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


4 entries were displayed.
```

6. Repeat these steps on the partner cluster.

Return to the ONTAP command-line interface and complete the MetroCluster configuration by performing the tasks that follow.

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.

Disabling automatic drive assignment (if doing manual assignment in ONTAP 9.4)

In ONTAP 9.4, if your MetroCluster IP configuration has fewer than four external storage shelves per site, you must disable automatic drive assignment on all nodes and manually assign drives.

About this task

This task is not required in ONTAP 9.5 and later.

This task does not apply to an AFF A800 system with an internal shelf and no external shelves.

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Steps

1. Disable automatic drive assignment:

   `storage disk option modify -node node_name -autoassign off`

   You need to issue this command on all nodes in the MetroCluster IP configuration.

Verifying drive assignment of pool 0 drives

You must verify that the remote drives are visible to the nodes and have been assigned correctly.

About this task

Automatic assignment depends on the storage system platform model and drive shelf arrangement.

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Steps

1. Verify that pool 0 drives are assigned automatically:

   `disk show`

   The following example shows the "cluster_A" output for an AFF A800 system with no external shelves.

   One quarter (8 drives) were automatically assigned to "node_A_1" and one quarter were automatically assigned to "node_A_2". The remaining drives will be remote (pool 1) drives for "node_B_1" and "node_B_2".

```
cluster_A::*> disk show
                 Usable     Disk      Container           Container
Disk             Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_A_1
```

```
node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_A_1
node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
```

```
32 entries were displayed.
```

The following example shows the "cluster_B" output:

```
cluster_B::> disk show
                 Usable     Disk              Container   Container
Disk             Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_B_1
node_B_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
```

```
node_B_2
node_B_2:0n.24   -           0      24  SSD-NVM unassigned  -          -
node_B_2:0n.25   -           0      25  SSD-NVM unassigned  -          -
node_B_2:0n.26   -           0      26  SSD-NVM unassigned  -          -
node_B_2:0n.27   -           0      27  SSD-NVM unassigned  -          -
node_B_2:0n.28   -           0      28  SSD-NVM unassigned  -          -
node_B_2:0n.29   -           0      29  SSD-NVM unassigned  -          -
node_B_2:0n.30   -           0      30  SSD-NVM unassigned  -          -
node_B_2:0n.31   -           0      31  SSD-NVM unassigned  -          -
node_B_2:0n.36   -           0      36  SSD-NVM unassigned  -          -
node_B_2:0n.37   -           0      37  SSD-NVM unassigned  -          -
node_B_2:0n.38   -           0      38  SSD-NVM unassigned  -          -
node_B_2:0n.39   -           0      39  SSD-NVM unassigned  -          -
node_B_2:0n.40   -           0      40  SSD-NVM unassigned  -          -
node_B_2:0n.41   -           0      41  SSD-NVM unassigned  -          -
node_B_2:0n.42   -           0      42  SSD-NVM unassigned  -          -
node_B_2:0n.43   -           0      43  SSD-NVM unassigned  -          -
32 entries were displayed.

cluster_B::>
```

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.

Related information

Cluster and SVM peering express configuration

Considerations when using dedicated ports

Considerations when sharing data ports

Configuring intercluster LIFs for cluster peering

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.

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.

The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                             Speed
(Mbps)
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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

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.

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

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

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`*

   The following example assigns ports "e0e" and "e0f" to the failover group "intercluster01" on the system "SVMcluster01":

   ```
   cluster01::> network interface failover-groups create -vserver cluster01
   -failover-group
   intercluster01 -targets
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

4. Verify that the failover group was created:

   `network interface failover-groups show`

   For complete command syntax, see the man page.

   ```
   cluster01::> network interface failover-groups show
                                     Failover
   Vserver          Group            Targets
   ---------------- ----------------
   --------------------------------------------
   Cluster
                    Cluster
                                     cluster01-01:e0a, cluster01-01:e0b,
                                     cluster01-02:e0a, cluster01-02:e0b
   cluster01
                    Default
                                     cluster01-01:e0c, cluster01-01:e0d,
                                     cluster01-02:e0c, cluster01-02:e0d,
                                     cluster01-01:e0e, cluster01-01:e0f
                                     cluster01-02:e0e, cluster01-02:e0f
                    intercluster01
                                     cluster01-01:e0e, cluster01-01:e0f
                                     cluster01-02:e0e, cluster01-02:e0f
   ```

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

ONTAP version	Command

9.6 and later	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover -group` *`failover_group`*
9.5 and earlier	`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.

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

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-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 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

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

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Related information

[Considerations when using dedicated ports](#)

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.

1. List the ports in the cluster:

   `network port show`

   For complete command syntax, see the man page.

   The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                                 Speed
(Mbps)
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:

In ONTAP 9.6 and later:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 and earlier:
`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.

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

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

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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:

In ONTAP 9.6 and later:
`network interface show –service-policy default-intercluster -failover`

In ONTAP 9.5 and earlier:

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

For complete command syntax, see the man page.

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

```
cluster01::> network interface show -service-policy default-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 information

Considerations when sharing data ports

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.

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.

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

```
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.

   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":

```
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`

```
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`

```
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
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

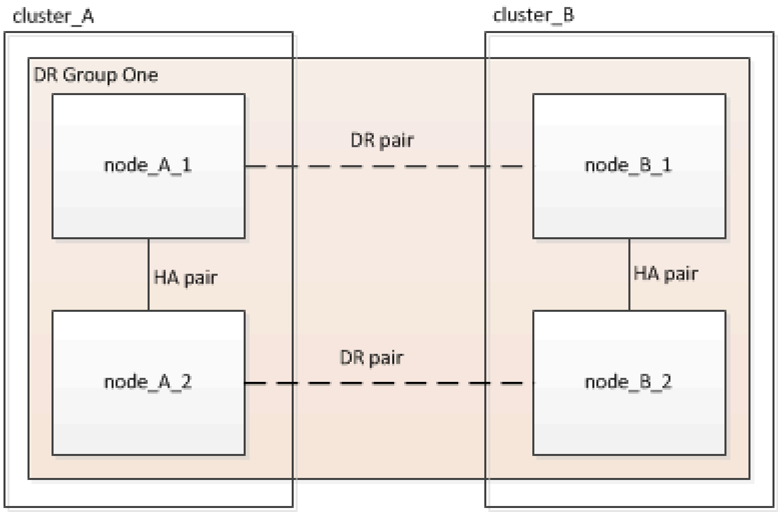
Creating the DR group

You must create the disaster recovery (DR) group relationships between the clusters.

About this task

You perform this procedure on one of the clusters in the MetroCluster configuration to create the DR relationships between the nodes in both clusters.

> The DR relationships cannot be changed after the DR groups are created.



Steps

1. Verify that the nodes are ready for creation of the DR group by entering the following command on each:

   `metrocluster configuration-settings show-status`

   The command output should show that the nodes are ready:

```
cluster_A::> metrocluster configuration-settings show-status
Cluster                    Node          Configuration Settings Status
-------------------------- -------------
--------------------------------
cluster_A                  node_A_1      ready for DR group create
                           node_A_2      ready for DR group create
2 entries were displayed.
```

```
cluster_B::> metrocluster configuration-settings show-status
Cluster                    Node          Configuration Settings Status
-------------------------- -------------
--------------------------------
cluster_B                  node_B_1      ready for DR group create
                           node_B_2      ready for DR group create
2 entries were displayed.
```

2. Create the DR group: `metrocluster configuration-settings dr-group create -partner -cluster` *`partner-cluster-name`* `-local-node` *`local-node-name`* `-remote-node` *`remote-node-name`*

This command is issued only once. It does not need to be repeated on the partner cluster. In the command, you specify the name of the remote cluster and the name of one local node and one node on the partner cluster.

The two nodes you specify are configured as DR partners and the other two nodes (which are not specified in the command) are configured as the second DR pair in the DR group. These relationships cannot be changed after you enter this command.

The following command creates these DR pairs:

- node_A_1 and node_B_1
- node_A_2 and node_B_2

```
Cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1
[Job 27] Job succeeded: DR Group Create is successful.
```

Configuring and connecting the MetroCluster IP interfaces

You must configure the MetroCluster IP interfaces that are used for replication of each node's storage and nonvolatile cache. You then establish the connections using the MetroCluster IP interfaces. This creates iSCSI connections for storage replication.

About this task

You must choose the MetroCluster IP addresses carefully because you cannot change them after initial configuration.

- You must create two interfaces for each node. The interfaces must be associated with the VLANs defined in the MetroCluster RCF file.
- You must create all MetroCluster IP interface "A" ports in the same VLAN and all MetroCluster IP interface "B" ports in the other VLAN. Refer to Considerations for MetroCluster IP configuration.

+

- Starting with ONTAP 9.8, certain platforms use a VLAN for the MetroCluster IP interface. By default, each of the two ports use a different VLAN: 10 and 20. You can also specify a different (non-default) VLAN higher than 100 (between 101 and 4095) using the `-vlan-id parameter` in the `metrocluster configuration-settings interface create` command.
- Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.

+ The following platform models use VLANs and allow configuration of a non-default VLAN ID.

+

AFF platforms	FAS platforms

• AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

The following IP addresses and subnets are used in the examples:

Node	Interface	IP address	Subnet
node_A_1	MetroCluster IP interface 1	10.1.1.1	10.1.1/24
	MetroCluster IP interface 2	10.1.2.1	10.1.2/24
node_A_2	MetroCluster IP interface 1	10.1.1.2	10.1.1/24
	MetroCluster IP interface 2	10.1.2.2	10.1.2/24
node_B_1	MetroCluster IP interface 1	10.1.1.3	10.1.1/24
	MetroCluster IP interface 2	10.1.2.3	10.1.2/24
node_B_2	MetroCluster IP interface 1	10.1.1.4	10.1.1/24
	MetroCluster IP interface 2	10.1.2.4	10.1.2/24

The physical ports used by the MetroCluster IP interfaces depends on the platform model, as shown in the following table.

Platform model	MetroCluster IP port	VLAN ID	

AFF A800	e0b	Not used	
	e1b		
AFF A700 and FAS9000	e5a		
	e5b		
AFF A400	e3a		
	e3b		
AFF A320	e0g		
	e0h		
AFF A300 and FAS8200	e1a		
	e1b		
AFF A220 and FAS2750	e0a	10	On these systems, these physical ports are also used as cluster interfaces.
	e0b	20	
AFF A250 and FAS500f	e0c	10	
	e0d	20	
FAS8300 and FAS8700	e0c		e0d

The port usage in the following examples is for an AFF A700 or a FAS9000 system.

1. Confirm that each node has disk automatic assignment enabled:

   `storage disk option show`

   Disk automatic assignment will assign pool 0 and pool 1 disks on a shelf-by-shelf basis.

   The Auto Assign column indicates whether disk automatic assignment is enabled.

```
Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on           on           on           default
node_A_2             on           on           on           default
2 entries were displayed.
```

2. Verify you can create MetroCluster IP interfaces on the nodes:

   `metrocluster configuration-settings show-status`

   All nodes should be ready:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for interface create
              node_A_2     ready for interface create
cluster_B
              node_B_1     ready for interface create
              node_B_2     ready for interface create
4 entries were displayed.
```

3. Create the interfaces on "node_A_1".

   - The port usage in the following examples is for an AFF A700 or a FAS9000 system (e5a and e5b). You must configure the interfaces on the correct ports for your platform model, as given above.
   - Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.
   - On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan-id` parameter if you don't want to use the default VLAN IDs.

   a. Configure the interface on port "e5a" on node_A_1:

      `metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

      The following example shows the creation of the interface on port "e5a" on "node_A_1" with IP address "10.1.1.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
10.1.1.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

   b. Configure the interface on port "e5b" on "node_A_1":

      `metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5b -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5b" on "node_A_1" with IP address "10.1.2.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

> You can verify that these interfaces are present using the `metrocluster configuration-settings interface show` command.

4. Create the interfaces on "node_A_2".

> - The port usage in the following examples is for an AFF A700 or a FAS9000 system (e5a and e5b). You must configure the interfaces on the correct ports for your platform model, as given above.
> - Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.
> - On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan-id` parameter if you don't want to use the default VLAN IDs.

a. Configure the interface on port "e5a" on "node_A_2":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5a" on "node_A_2" with IP address "10.1.1.2":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e5a -address
10.1.1.2 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan -id` paramter if you don't want to use the default VLAN IDs. The following example shows the command for an AFF A220 system with a VLAN ID of "120":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

b. Configure the interface on port "e5b" on "node_A_2":

`metrocluster configuration-settings interface create -cluster-name *cluster-name* -home-node *node-name* -home-port e5b -address *ip-address* -netmask *netmask*`

The following example shows the creation of the interface on port "e5b" on "node_A_2" with IP address "10.1.2.2":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e5b -address
10.1.2.2 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan -id` paramter if you don't want to use the default VLAN IDs. The following example shows the command for an AFF A220 system with a VLAN ID of "220":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0b -address
10.1.2.2 -netmask 255.255.255.0 -vlan-id 220
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

5. Create the interfaces on "node_B_1".

> ◦ The port usage in the following examples is for an AFF A700 or a FAS9000 system (e5a and e5b). You must configure the interfaces on the correct ports for your platform model, as given above.
>
> ◦ Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.
>
> ◦ On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan-id` parameter if you don't want to use the default VLAN IDs.

a. Configure the interface on port "e5a on "node_B_1":

`metrocluster configuration-settings interface create -cluster-name *cluster-*`

```
name -home-node node-name -home-port e5a -address ip-address -netmask
netmask
```

The following example shows the creation of the interface on port "e5a" on "node_B_1" with IP address "10.1.1.3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_B_1 -home-port e5a -address
10.1.1.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Configure the interface on port "e5b" on "node_B_1":

```
metrocluster configuration-settings interface create -cluster-name cluster-
name -home-node node-name -home-port e5a -address ip-address -netmask
netmask
```

The following example shows the creation of the interface on port "e5b" on "node_B_1" with IP address "10.1.2.3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_B_1 -home-port e5b -address
10.1.2.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

6. Create the interfaces on "node_B_2".

   - The port usage in the following examples is for an AFF A700 or a FAS9000 system (e5a and e5b). You must configure the interfaces on the correct ports for your platform model, as given above.
   - Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.
   - On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan-id` parameter if you don't want to use the default VLAN IDs.

a. Configure the interface on port "e5a" on "node_B_2":

```
metrocluster configuration-settings interface create -cluster-name cluster-
name -home-node node-name -home-port e5a -address ip-address -netmask
netmask
```

The following example shows the creation of the interface on port "e5a" on "node_B_2" with IP address "10.1.1.4":

```
cluster_B::>metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address
10.1.1.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Configure the interface on port "e5b" on "node_B_2":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5b -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5b" on "node_B_2" with IP address "10.1.2.4":

```
cluster_B::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address
10.1.2.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

7. Verify that the interfaces have been configured:

`metrocluster configuration-settings interface show`

The following example shows that the configuration state for each interface is completed.

```
cluster_A::> metrocluster configuration-settings interface show
DR                                                                  Config
Group Cluster Node    Network Address Netmask         Gateway   State
----- ------- ------- --------------- --------------- ---------
----------
1     cluster_A  node_A_1
                 Home Port: e5a
                      10.1.1.1     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.1     255.255.255.0   -         completed
                 node_A_2
                 Home Port: e5a
                      10.1.1.2     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.2     255.255.255.0   -         completed
      cluster_B  node_B_1
                 Home Port: e5a
                      10.1.1.3     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.3     255.255.255.0   -         completed
                 node_B_2
                 Home Port: e5a
                      10.1.1.4     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.4     255.255.255.0   -         completed
8 entries were displayed.
cluster_A::>
```

8. Verify that the nodes are ready to connect the MetroCluster interfaces:

   `metrocluster configuration-settings show-status`

   The following example shows all nodes in the "ready for connection" state:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for connection connect
              node_A_2     ready for connection connect
cluster_B
              node_B_1     ready for connection connect
              node_B_2     ready for connection connect
4 entries were displayed.
```

9. Establish the connections:

   `metrocluster configuration-settings connection connect`

   The IP addresses cannot be changed after you issue this command.

   The following example shows "cluster_A" is successfully connected:

```
cluster_A::> metrocluster configuration-settings connection connect
[Job 53] Job succeeded: Connect is successful.
cluster_A::>
```

10. Verify that the connections have been established:

    `metrocluster configuration-settings show-status`

    The configuration settings status for all nodes should be completed:

```
Cluster       Node          Configuration Settings Status
----------    -----------   ---------------------------------
cluster_A
              node_A_1      completed
              node_A_2      completed
cluster_B
              node_B_1      completed
              node_B_2      completed
4 entries were displayed.
```

11. Verify that the iSCSI connections have been established:

    a. 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. Display the connections:

       `storage iscsi-initiator show`

       On systems running ONTAP 9.5, there are eight MetroCluster IP initiators on each cluster that should appear in the output.

       On systems running ONTAP 9.4 and earlier, there are four MetroCluster IP initiators on each cluster that should appear in the output.

       The following example shows the eight MetroCluster IP initiators on a cluster running ONTAP 9.5:

```
cluster_A::*> storage iscsi-initiator show
Node Type Label    Target Portal           Target Name
Admin/Op
---- ---- -------- ------------------
------------------------------- --------

cluster_A-01
     dr_auxiliary
              mccip-aux-a-initiator
                   10.227.16.113:65200     prod506.com.company:abab44
up/up
              mccip-aux-a-initiator2
                   10.227.16.113:65200     prod507.com.company:abab44
up/up
              mccip-aux-b-initiator
                   10.227.95.166:65200     prod506.com.company:abab44
up/up
              mccip-aux-b-initiator2
                   10.227.95.166:65200     prod507.com.company:abab44
up/up
     dr_partner
              mccip-pri-a-initiator
                   10.227.16.112:65200     prod506.com.company:cdcd88
up/up
              mccip-pri-a-initiator2
                   10.227.16.112:65200     prod507.com.company:cdcd88
up/up
              mccip-pri-b-initiator
                   10.227.95.165:65200     prod506.com.company:cdcd88
up/up
              mccip-pri-b-initiator2
                   10.227.95.165:65200     prod507.com.company:cdcd88
up/up
cluster_A-02
     dr_auxiliary
              mccip-aux-a-initiator
                   10.227.16.112:65200     prod506.com.company:cdcd88
up/up
              mccip-aux-a-initiator2
                   10.227.16.112:65200     prod507.com.company:cdcd88
up/up
              mccip-aux-b-initiator
                   10.227.95.165:65200     prod506.com.company:cdcd88
up/up
              mccip-aux-b-initiator2
                   10.227.95.165:65200     prod507.com.company:cdcd88
```

```
up/up
     dr_partner
              mccip-pri-a-initiator
                   10.227.16.113:65200     prod506.com.company:abab44
up/up
              mccip-pri-a-initiator2
                   10.227.16.113:65200     prod507.com.company:abab44
up/up
              mccip-pri-b-initiator
                   10.227.95.166:65200     prod506.com.company:abab44
up/up
              mccip-pri-b-initiator2
                   10.227.95.166:65200     prod507.com.company:abab44
up/up
16 entries were displayed.
```

c. Return to the admin privilege level:

`set -privilege admin`

12. Verify that the nodes are ready for final implementation of the MetroCluster configuration:

`metrocluster node show`

```
cluster_A::> metrocluster node show
DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_A
              node_A_1           ready to configure -     -
              node_A_2           ready to configure -     -
2 entries were displayed.
cluster_A::>
```

```
cluster_B::> metrocluster node show
DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_B
              node_B_1           ready to configure -     -
              node_B_2           ready to configure -     -
2 entries were displayed.
cluster_B::>
```

Verifying or manually performing pool 1 drives assignment

Depending on the storage configuration, you must either verify pool 1 drive assignment or manually assign drives to pool 1 for each node in the MetroCluster IP configuration.

About this task

The procedure you use depends on the version of ONTAP you are using.

Configuration type	Procedure
The systems meet the requirements for automatic drive assignment or, if running ONTAP 9.3, were received from the factory.	Verifying disk assignment for pool 1 disks
The configuration includes either three shelves, or, if it contains more than four shelves, has an uneven multiple of four shelves (for example, seven shelves), and is running ONTAP 9.5.	Manually assigning drives for pool 1 (ONTAP 9.4 or later)
The configuration does not include four storage shelves per site and is running ONTAP 9.4	Manually assigning drives for pool 1 (ONTAP 9.4 or later)
The systems were not received from the factory and are running ONTAP 9.3Systems received from the factory are pre-configured with assigned drives.	Manually assigning disks for pool 1 (ONTAP 9.3)

Verifying disk assignment for pool 1 disks

You must verify that the remote disks are visible to the nodes and have been assigned correctly.

About this task

You must wait at least ten minutes for disk auto-assignment to complete after the MetroCluster IP interfaces and connections were created with the `metrocluster configuration-settings connection connect` command.

Command output will show disk names in the following format:

`node-name:0m.i1.0L1`

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Step

1. Verify that pool 1 disks are auto-assigned:

   `disk show`

   The following output shows the output for an AFF A800 system with no external shelves.

   Drive autoassignment has assigned one quarter (8 drives) to "node_A_1" and one quarter to "node_A_2". The remaining drives will be remote (pool1) disks for "node_B_1" and "node_B_2".

```
cluster_B::> disk show -host-adapter 0m -owner node_B_2
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_2:0m.i0.2L4  894.0GB    0     29  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.2L10 894.0GB    0     25  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L3  894.0GB    0     28  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L9  894.0GB    0     24  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L11 894.0GB    0     26  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L12 894.0GB    0     27  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L15 894.0GB    0     30  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L16 894.0GB    0     31  SSD-NVM shared      -
node_B_2
8 entries were displayed.

cluster_B::> disk show -host-adapter 0m -owner node_B_1
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i2.3L19 1.75TB     0     42  SSD-NVM shared      -
node_B_1
node_B_1:0m.i2.3L20 1.75TB     0     43  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L23 1.75TB     0     40  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L24 1.75TB     0     41  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L29 1.75TB     0     36  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L30 1.75TB     0     37  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L31 1.75TB     0     38  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L32 1.75TB     0     39  SSD-NVM shared       -
node_B_1
```

```
8 entries were displayed.

cluster_B::> disk show
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i1.0L6  1.75TB     0     1   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L8  1.75TB     0     3   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L17 1.75TB     0     18  SSD-NVM shared      -
node_A_1
node_B_1:0m.i1.0L22 1.75TB     0     17 SSD-NVM shared - node_A_1
node_B_1:0m.i1.0L25 1.75TB     0     12 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L2  1.75TB     0     5 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L7  1.75TB     0     2 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L14 1.75TB     0     7 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L21 1.75TB     0     16 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L27 1.75TB     0     14 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L28 1.75TB     0     15 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L1  1.75TB     0     4 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L5  1.75TB     0     0 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L13 1.75TB     0     6 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L18 1.75TB     0     19 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L26 1.75TB     0     13 SSD-NVM shared - node_A_1
node_B_1:0m.i2.3L19 1.75TB     0 42 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L20 1.75TB     0 43 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L23 1.75TB     0 40 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L24 1.75TB     0 41 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L29 1.75TB     0 36 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L30 1.75TB     0 37 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L31 1.75TB     0 38 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L32 1.75TB     0 39 SSD-NVM shared - node_B_1
node_B_1:0n.12      1.75TB     0 12 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.13      1.75TB     0 13 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.14      1.75TB     0 14 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.15      1.75TB 0 15 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.16      1.75TB 0 16 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.17      1.75TB 0 17 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.18      1.75TB 0 18 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.19      1.75TB 0 19 SSD-NVM shared - node_B_1
node_B_1:0n.24      894.0GB 0 24 SSD-NVM shared - node_A_2
node_B_1:0n.25      894.0GB 0 25 SSD-NVM shared - node_A_2
node_B_1:0n.26      894.0GB 0 26 SSD-NVM shared - node_A_2
```

```
node_B_1:0n.27      894.0GB 0 27 SSD-NVM shared - node_A_2
node_B_1:0n.28      894.0GB 0 28 SSD-NVM shared - node_A_2
node_B_1:0n.29      894.0GB 0 29 SSD-NVM shared - node_A_2
node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4  894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3  894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9  894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0       1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

cluster_B::>


cluster_A::> disk show
Usable Disk Container Container
Disk Size Shelf Bay Type Type Name Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
```

```
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
```

```
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>
```

Manually assigning drives for pool 1 (ONTAP 9.4 or later)

If the system was not preconfigured at the factory and does not meet the requirements for automatic drive assignment, you must manually assign the remote pool 1 drives.

About this task

This procedure applies to configurations running ONTAP 9.4 or later.

Details for determining whether your system requires manual disk assignment are included in Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later.

When the configuration includes only two external shelves per site, pool 1 drives for each site should be shared from the same shelf as shown in the following examples:

- node_A_1 is assigned drives in bays 0-11 on site_B-shelf_2 (remote)
- node_A_2 is assigned drives in bays 12-23 on site_B-shelf_2 (remote)

Steps

1. From each node in the MetroCluster IP configuration, assign remote drives to pool 1.
   a. Display the list of unassigned drives:

      ```
      disk show -host-adapter 0m -container-type unassigned
      ```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Assign ownership of remote drives (0m) to pool 1 of the first node (for example, "node_A_1"):

`disk assign -disk` *`disk-id`* `-pool 1 -owner` *`owner-node-name`*

The `disk-id` must identify a drive on a remote shelf of `owner-node-name`.

c. Confirm that the drives were assigned to pool 1:

`disk show -host-adapter 0m -container-type unassigned`

The iSCSI connection used to access the remote drives appears as device 0m.

The following output shows that the drives on shelf "23" were assigned because they no longer appear in the list of unassigned drives:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

d. Repeat these steps to assign pool 1 drives to the second node on site A (for example, "n"ode_A_2").

e. Repeat these steps on site B.

Manually assigning disks for pool 1 (ONTAP 9.3)

If you have at least two disk shelves for each node, you use ONTAP's auto-assignment functionality to automatically assign the remote (pool 1) disks.

About this task

You must first assign a disk on the shelf to pool 1. ONTAP then automatically assigns the rest of the disks on the shelf to the same pool.

This procedure applies to configurations running ONTAP 9.3.

This procedure can be used only if you have at least two disk shelves for each node, which allows shelf-level auto-assignment of disks.

If you cannot use shelf-level auto-assignment, you must manually assign your remote disks so that each node has a remote pool of disks (pool 1).

The ONTAP automatic disk assignment feature assigns the disks on a shelf-by-shelf basis. For example:

- All the disks on site_B-shelf_2 are autoassigned to pool1 of node_A_1
- All the disks on site_B-shelf_4 are autoassigned to pool1 of node_A_2
- All the disks on site_A-shelf_2 are autoassigned to pool1 of node_B_1
- All the disks on site_A-shelf_4 are autoassigned to pool1 of node_B_2

You must "seed" the auto-assignment by specifying a single disk on each shelf.

Steps

1. From each node in the MetroCluster IP configuration, assign a remote disk to pool 1.
   a. Display the list of unassigned disks:

```
disk show -host-adapter 0m -container-type unassigned
```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Select a remote disk (0m) and assign ownership of the disk to pool 1 of the first node (for example, "node_A_1"):

```
disk assign -disk disk-id -pool 1 -owner owner-node-name
```

The `disk-id` must identify a disk on a remote shelf of `owner-node-name`.

The ONTAP disk auto-assignment feature assigns all disks on the remote shelf that contains the specified disk.

c. After waiting at least 60 seconds for disk auto-assignment to take place, verify that the remote disks on the shelf were auto-assigned to pool 1:

```
disk show -host-adapter 0m -container-type unassigned
```

> The iSCSI connection used to access the remote disks appears as device 0m.

The following output shows that the disks on shelf "23" have now been assigned and no longer appear:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk     Container   Container
Disk                   Size Shelf Bay Type     Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
node_A_2:0m.i1.2L72       -    21  23 SSD     unassigned  -         -
node_A_2:0m.i1.2L74       -    21   1 SSD     unassigned  -         -
node_A_2:0m.i1.2L83       -    21  22 SSD     unassigned  -         -
node_A_2:0m.i1.2L90       -    21   7 SSD     unassigned  -         -
node_A_2:0m.i1.3L52       -    21   6 SSD     unassigned  -         -
node_A_2:0m.i1.3L59       -    21  13 SSD     unassigned  -         -
node_A_2:0m.i1.3L66       -    21  17 SSD     unassigned  -         -
node_A_2:0m.i1.3L73       -    21  12 SSD     unassigned  -         -
node_A_2:0m.i1.3L80       -    21   5 SSD     unassigned  -         -
node_A_2:0m.i1.3L81       -    21   2 SSD     unassigned  -         -
node_A_2:0m.i1.3L82       -    21  16 SSD     unassigned  -         -
node_A_2:0m.i1.3L91       -    21   3 SSD     unassigned  -         -
node_A_2:0m.i2.0L49       -    21  15 SSD     unassigned  -         -
node_A_2:0m.i2.0L50       -    21   4 SSD     unassigned  -         -
node_A_2:0m.i2.1L57       -    21  18 SSD     unassigned  -         -
node_A_2:0m.i2.1L58       -    21  11 SSD     unassigned  -         -
node_A_2:0m.i2.1L59       -    21  21 SSD     unassigned  -         -
node_A_2:0m.i2.1L65       -    21  20 SSD     unassigned  -         -
node_A_2:0m.i2.1L72       -    21   9 SSD     unassigned  -         -
node_A_2:0m.i2.1L80       -    21   0 SSD     unassigned  -         -
node_A_2:0m.i2.1L88       -    21   8 SSD     unassigned  -         -
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

d. Repeat these steps to assign pool 1 disks to the second node on site A (for example, "node_A_2").
e. Repeat these steps on site B.

Enabling automatic drive assignment in ONTAP 9.4

In ONTAP 9.4, if you disabled automatic drive assignment as directed previously in this procedure, you must reenable it on all nodes.

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Step

1. Enable automatic drive assignment:

`storage disk option modify -node node_name -autoassign on`

You must issue this command on all nodes in the MetroCluster IP configuration.

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`

> 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`

   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

Creating a mirrored data aggregate on each node

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

About this task

- You should know what drives 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.
- Drives 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.

  In systems using ADP, aggregates are created using partitions in which each drive is partitioned in to P1, P2 and P3 partitions.
- 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:

   `storage aggregate create -mirror true`

   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 that are to be added to the aggregate.
   - Number of drives to include.

     > 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 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.

     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
```

Implementing the MetroCluster configuration

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

About this task

- There should be at least two non-root mirrored data aggregates on each cluster.

  You can verify this with the storage aggregate show command.

  > If you want to use a single mirrored data aggregate, then see Step 1 for instructions.

- The ha-config state of the controllers and chassis must be mccip.

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.

The `metrocluster configure` command automatically pairs the two nodes with the lowest system IDs in each of the two clusters as disaster recovery (DR) partners. In a four-node MetroCluster configuration, there are two DR partner pairs. The second DR pair is created from the two nodes with higher system IDs.

Steps

1. Configure the MetroCluster in the following format:

If your MetroCluster configuration has…	Then do this…
Multiple data aggregates	From any node's prompt, configure MetroCluster: `metrocluster configure node-name`

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`

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":

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

[Job 121] Job succeeded: Configure is successful.
```

2. Verify the networking status on site A: `network port show`

   The following example shows the network port usage on a four-node MetroCluster configuration:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

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

   a. Verify the configuration from site A:

      `metrocluster show`

```
cluster_A::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
Remote: cluster_B         Configuration state configured
                          Mode                normal
```

b. Verify the configuration from site B:

`metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

4. To avoid possible issues with nonvolatile memory mirroring, reboot each of the four nodes:

   `node reboot -node` *`node-name`* `-inhibit-takeover true`

5. Issue the `metrocluster show` command on both clusters to again verify the configuration.

Configuring the second DR group in an eight-node configuration

Repeat the previous tasks to configure the nodes in the second DR group.

Creating unmirrored data aggregates

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

About this task

- 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.

> In MetroCluster IP configurations, remote unmirrored aggregates are not accessible after a switchover

> 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. Enable unmirrored aggregate deployment:

   `metrocluster modify -enable-unmirrored-aggr-deployment true`

2. Verify that disk auto-assignment is disabled:

   `disk option show`

3. Install and cable the disk shelves that will contain the unmirrored aggregates.

   You can use the procedures in the *Installation and Setup* documentation for your platform and disk shelves.

   [AFF and FAS Documentation Center]

4. Manually assign all disks on the new shelf to the appropriate node:

   `disk assign -disk disk-id -owner owner-node-name`

5. Create the aggregate:

   `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 must also ensure that you are only including drives on the unmirrored shelf to the aggregate.

   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.

  The following command creates a unmirrored aggregate with 10 disks:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

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

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

7. Disable unmirrored aggregate deployment:

   `metrocluster modify -enable-unmirrored-aggr-deployment false`

8. Verify that disk autoassignment is enabled:

   `disk option show`

Related information

Disk and aggregate management

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`

   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: 9/13/2018 20:41:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
6 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.

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

Node                  Aggregate                  Check
```

```
Result
---------------      --------------------       ---------------------
---------
controller_A_1       controller_A_1_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                     controller_A_1_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                     controller_A_1_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok


controller_A_2       controller_A_2_aggr0
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                     controller_A_2_aggr1
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
ok
                     controller_A_2_aggr2
                                                mirroring-status
ok
                                                disk-pool-allocation
ok
                                                ownership-state
```

```
ok

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

Cluster               Check                           Result
--------------------- ------------------------------- ---------
mccint-fas9000-0102
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
mccint-fas9000-0304
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
10 entries were displayed.
```

Related information

Disk and aggregate management

Network and LIF management

Completing ONTAP configuration

After configuring, enabling, and checking the MetroCluster configuration, you can proceed to complete the cluster configuration by adding additional SVMs, network interfaces and other ONTAP functionality as needed.

Verifying switchover, healing, and switchback

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

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

Configuring the MetroCluster Tiebreaker or ONTAP Mediator software

You can download and install on a third site either the MetroCluster Tiebreaker software, or, starting with ONTAP 9.7, the ONTAP Mediator.

Before you begin

You must have a Linux host available that has network connectivity to both clusters in the MetroCluster configuration. The specific requirements are in the MetroCluster Tiebreaker or ONTAP Mediator documentation.

If you are connecting to an existing Tiebreaker or ONTAP Mediator instance, you need the username, password, and IP address of the Tiebreaker or Mediator service.

If you must install a new instance of the ONTAP Mediator, follow the directions to install and configure the software.

Configuring the ONTAP Mediator service for unplanned automatic switchover

If you must install a new instance of the Tiebreaker software, follow the directions to install and configure the software.

MetroCluster Tiebreaker Software Installation and Configuration Guide

About this task

You cannot use both the MetroCluster Tiebreaker software and the ONTAP Mediator with the same MetroCluster configuration.

Considerations for using ONTAP Mediator or MetroCluster Tiebreaker

Steps

1. Configure the ONTAP Mediator service or the Tiebreaker software:
   - If you are using an existing instance of the ONTAP Mediator, add the ONTAP Mediator service to ONTAP:

     `metrocluster configuration-settings mediator add -mediator-address` *`ip-address-of-mediator-host`*

   - If you are using the Tiebreaker software, refer to the Tiebreaker documentation.

     MetroCluster Tiebreaker Software Installation and Configuration Guide

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.

Steps

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*.

Related information

System administration

Restoring system defaults on a controller module

Reset and restore defaults on the controller modules.

1. At the LOADER prompt, return environmental variables to their default setting: `set-defaults`
2. Boot the node to the boot menu: `boot_ontap menu`

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

3. Clear the node configuration:

   - If you are using systems configured for ADP, select option `9a` from the boot menu, and respond `yes` when prompted.

     > ⓘ This process is disruptive.

     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)?  9a
########## WARNING ##########

    This is a disruptive operation and will result in the
    loss of all filesystem data. Before proceeding further,
    make sure that:
    1) This option (9a) has been executed or will be executed
    on the HA partner node, prior to reinitializing either
    system in the HA-pair.
    2) The HA partner node is currently in a halted state or
    at the LOADER prompt.


    Do you still want to continue (yes/no)? yes
```

- If your system is not configured for ADP, type `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.
```

Manually assigning drives to pool 0

If you did not receive the systems pre-configured from the factory, you might have to manually assign the pool 0 drives. Depending on the platform model and whether the system is using ADP, you must manually assign drives to pool 0 for each node in the MetroCluster IP configuration. The procedure you use depends on the version of ONTAP you are using.

Manually assigning drives for pool 0 (ONTAP 9.4 and later)

If the system has not been pre-configured at the factory and does not meet the requirements for automatic drive assignment, you must manually assign the pool 0 drives.

About this task

This procedure applies to configurations running ONTAP 9.4 or later.

To determine if your system requires manual disk assignment, you should review Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later.

You perform these steps in Maintenance mode. The procedure must be performed on each node in the configuration.

Examples in this section are based on the following assumptions:

- node_A_1 and node_A_2 own drives on:
  - site_A-shelf_1 (local)
  - site_B-shelf_2 (remote)

* node_B_1 and node_B_2 own drives on:
  * site_B-shelf_1 (local)
  * site_A-shelf_2 (remote)

Steps

1. Display the boot menu:

   ```
   boot_ontap menu
   ```

2. Select option 9a.

   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)?  9a
   ########## WARNING ##########

       This is a disruptive operation and will result in the
       loss of all filesystem data. Before proceeding further,
       make sure that:
       1) This option (9a) has been executed or will be executed
       on the HA partner node (and DR/DR-AUX partner nodes if
       applicable), prior to reinitializing any system in the
       HA-pair (or MetroCluster setup).
       2) The HA partner node (and DR/DR-AUX partner nodes if
       applicable) is currently waiting at the boot menu.

       Do you still want to continue (yes/no)? yes
   ```

3. When the node restarts, press Ctrl-C when prompted to display the boot menu and then select the option for **Maintenance mode boot**.

4. In Maintenance mode, manually assign drives for the local aggregates on the node:

   `disk assign` *`disk-id`* `-p 0 -s` *`local-node-sysid`*

   The drives should be assigned symmetrically, so each node has an equal number of drives. The following steps are for a configuration with two storage shelves at each site.

a. When configuring node_A_1, manually assign drives from slot 0 to 11 to pool0 of node A1 from site_A-shelf_1.
b. When configuring node_A_2, manually assign drives from slot 12 to 23 to pool0 of node A2 from site_A-shelf_1.
c. When configuring node_B_1, manually assign drives from slot 0 to 11 to pool0 of node B1 from site_B-shelf_1.
d. When configuring node_B_2, manually assign drives from slot 12 to 23 to pool0 of node B2 from site_B-shelf_1.

5. Exit Maintenance mode:

```
halt
```

6. Display the boot menu:

```
boot_ontap menu
```

7. Select option "4" from the boot menu and let the system boot.
8. Repeat these steps on the other nodes in the MetroCluster IP configuration.
9. Proceed to Setting up ONTAP.

Manually assigning drives for pool 0 (ONTAP 9.3)

If you have at least two disk shelves for each node, you use ONTAP's auto-assignment functionality to automatically assign the local (pool 0) disks.

About this task

While the node is in Maintenance mode, you must first assign a single disk on the appropriate shelves to pool 0. ONTAP then automatically assigns the rest of the disks on the shelf to the same pool. This task is not required on systems received from the factory, which have pool 0 to contain the pre-configured root aggregate.

This procedure applies to configurations running ONTAP 9.3.

This procedure is not required if you received your MetroCluster configuration from the factory. Nodes from the factory are configured with pool 0 disks and root aggregates.

This procedure can be used only if you have at least two disk shelves for each node, which allows shelf-level autoassignment of disks. If you cannot use shelf-level autoassignment, you must manually assign your local disks so that each node has a local pool of disks (pool 0).

These steps must be performed in Maintenance mode.

Examples in this section assume the following disk shelves:

- node_A_1 owns disks on:
  - site_A-shelf_1 (local)
  - site_B-shelf_2 (remote)
- node_A_2 is connected to:
  - site_A-shelf_3 (local)
  - site_B-shelf_4 (remote)

- node_B_1 is connected to:
  - site_B-shelf_1 (local)
  - site_A-shelf_2 (remote)
- node_B_2 is connected to:
  - site_B-shelf_3 (local)
  - site_A-shelf_4 (remote)

Steps

1. Manually assign a single disk for root aggregate on each node:

   `disk assign` *`disk-id`* `-p 0 -s` *`local-node-sysid`*

   The manual assignment of these disks allows the ONTAP autoassignment feature to assign the rest of the disks on each shelf.

   a. On node_A_1, manually assign one disk from local site_A-shelf_1 to pool 0.
   b. On node_A_2, manually assign one disk from local site_A-shelf_3 to pool 0.
   c. On node_B_1, manually assign one disk from local site_B-shelf_1 to pool 0.
   d. On node_B_2, manually assign one disk from local site_B-shelf_3 to pool 0.
2. Boot each node at site A, using option 4 on the boot menu:

   You should complete this step on a node before proceeding to the next node.

   a. Exit Maintenance mode:

      `halt`

   b. Display the boot menu:

      `boot_ontap menu`

   c. Select option 4 from the boot menu and proceed.
3. Boot each node at site B, using option 4 on the boot menu:

   You should complete this step on a node before proceeding to the next node.

   a. Exit Maintenance mode:

      `halt`

   b. Display the boot menu:

      `boot_ontap menu`

   c. Select option 4 from the boot menu and proceed.

Setting up ONTAP

After you boot each node, you are prompted to perform basic node and cluster configuration. After configuring the cluster, you return to the ONTAP CLI to create aggregates and create the MetroCluster configuration.

Before you begin

- You must have cabled the MetroCluster configuration.
- You must not have configured the Service Processor.

If you need to netboot the new controllers, see Netbooting the new controller modules.

About this task

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

Steps

1. Power up each node at the local site if you have not already done so and let them all boot completely.

   If the system is in Maintenance mode, you need to issue the halt command to exit Maintenance mode, and then issue the `boot_ontap` command to boot the system and get to cluster setup.

2. On the first node in each cluster, proceed through the prompts to configure the cluster.
   a. Enable the AutoSupport tool by following the directions provided by the system.

      The output should be similar to the following:

```
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.

    This system will send event messages and periodic 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}: yes
.
.
.
```

b. Configure the node management interface by responding to the prompts.

   The prompts are similar to the following:

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.229
has been created.
```

c. Create the cluster by responding to the prompts.

   The prompts are similar to the following:

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


Do you intend for this node to be used as a single node cluster?
{yes, no} [no]:
no

Existing cluster interface configuration found:

Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]: no

Enter the cluster administrator's (username "admin") password:

Retype the password:


Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.

List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A

Creating cluster cluster_A

Starting cluster support services ...

Cluster cluster_A has been created.
```

d. Add licenses, set up a Cluster Administration SVM, and enter DNS information by responding to the prompts.

   The prompts are similar to the following:

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:


Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.


Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

e. Enable storage failover and set up the node by responding to the prompts.

   The prompts are similar to the following:

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: site_A
```

f. Complete the configuration of the node, but do not create data aggregates.

   You can use ONTAP System Manager, pointing your web browser to the cluster management IP address (https://172.17.12.153).

   Cluster management using System Manager (Versions 9.0 to 9.6)

   ONTAP System Manager (Version 9.7 and later)

3. Boot the next controller and join it to the cluster, following the prompts.
4. Confirm that nodes are configured in high-availability mode:

   `storage failover show -fields mode`

   If not, you must configure HA mode on each node, and then reboot the nodes:

   `storage failover modify -mode ha -node localhost`

   This command configures high-availability mode but does not enable storage failover. Storage failover is automatically enabled when you configure the MetroCluster configuration later in the process.

5. Confirm that you have four ports configured as cluster interconnects:

   `network port show`

   The MetroCluster IP interfaces are not configured at this time and do not appear in the command output.

   The following example shows two cluster ports on node_A_1:

```
cluster_A::*> network port show -role cluster



Node: node_A_1


Ignore
```

```
                                                   Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


Node: node_A_2


Ignore

                                                   Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


4 entries were displayed.
```

6. Repeat these steps on the partner cluster.

What to do next

Return to the ONTAP command-line interface and complete the MetroCluster configuration by performing the tasks that follow.

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.

Disabling automatic drive assignment (if doing manual assignment in ONTAP 9.4)

In ONTAP 9.4, if your MetroCluster IP configuration has fewer than four external storage shelves per site, you must disable automatic drive assignment on all nodes and manually assign drives.

About this task

This task is not required in ONTAP 9.5 and later.

This task does not apply to an AFF A800 system with an internal shelf and no external shelves.

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Steps

1. Disable automatic drive assignment:

   `storage disk option modify -node node_name -autoassign off`

2. You need to issue this command on all nodes in the MetroCluster IP configuration.

Verifying drive assignment of pool 0 drives

You must verify that the remote drives are visible to the nodes and have been assigned correctly.

About this task

Automatic assignment depends on the storage system platform model and drive shelf arrangement.

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Steps

1. Verify that pool 0 drives are assigned automatically:

   `disk show`

   The following example shows the "cluster_A" output for an AFF A800 system with no external shelves.

   One quarter (8 drives) were automatically assigned to "node_A_1" and one quarter were automatically assigned to "node_A_2". The remaining drives will be remote (pool 1) drives for "node_B_1" and "node_B_2".

```
cluster_A::*> disk show
                  Usable      Disk      Container           Container
Disk              Size        Shelf Bay Type     Type         Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0n.12    1.75TB      0     12  SSD-NVM shared       aggr0
```

```
node_A_1
node_A_1:0n.13   1.75TB      0      13  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.14   1.75TB      0      14  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.15   1.75TB      0      15  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.16   1.75TB      0      16  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.17   1.75TB      0      17  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.18   1.75TB      0      18  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.19   1.75TB      0      19  SSD-NVM shared      -
node_A_1
node_A_2:0n.0    1.75TB      0      0   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.1    1.75TB      0      1   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.2    1.75TB      0      2   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.3    1.75TB      0      3   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.4    1.75TB      0      4   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.5    1.75TB      0      5   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6    1.75TB      0      6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB      0      7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -           0      24  SSD-NVM unassigned  -          -
node_A_2:0n.25   -           0      25  SSD-NVM unassigned  -          -
node_A_2:0n.26   -           0      26  SSD-NVM unassigned  -          -
node_A_2:0n.27   -           0      27  SSD-NVM unassigned  -          -
node_A_2:0n.28   -           0      28  SSD-NVM unassigned  -          -
node_A_2:0n.29   -           0      29  SSD-NVM unassigned  -          -
node_A_2:0n.30   -           0      30  SSD-NVM unassigned  -          -
node_A_2:0n.31   -           0      31  SSD-NVM unassigned  -          -
node_A_2:0n.36   -           0      36  SSD-NVM unassigned  -          -
node_A_2:0n.37   -           0      37  SSD-NVM unassigned  -          -
node_A_2:0n.38   -           0      38  SSD-NVM unassigned  -          -
node_A_2:0n.39   -           0      39  SSD-NVM unassigned  -          -
node_A_2:0n.40   -           0      40  SSD-NVM unassigned  -          -
node_A_2:0n.41   -           0      41  SSD-NVM unassigned  -          -
node_A_2:0n.42   -           0      42  SSD-NVM unassigned  -          -
```

```
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

The following example shows the "cluster_B" output:

```
cluster_B::> disk show
                 Usable     Disk                 Container   Container
Disk             Size       Shelf Bay Type       Type        Name
Owner
---------------- ---------- ----- --- -------   ----------- ---------
--------

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_B_1
node_B_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
```

```
node_B_2:0n.7     1.75TB      0      7   SSD-NVM shared       -
node_B_2
node_B_2:0n.24    -           0      24  SSD-NVM unassigned   -          -
node_B_2:0n.25    -           0      25  SSD-NVM unassigned   -          -
node_B_2:0n.26    -           0      26  SSD-NVM unassigned   -          -
node_B_2:0n.27    -           0      27  SSD-NVM unassigned   -          -
node_B_2:0n.28    -           0      28  SSD-NVM unassigned   -          -
node_B_2:0n.29    -           0      29  SSD-NVM unassigned   -          -
node_B_2:0n.30    -           0      30  SSD-NVM unassigned   -          -
node_B_2:0n.31    -           0      31  SSD-NVM unassigned   -          -
node_B_2:0n.36    -           0      36  SSD-NVM unassigned   -          -
node_B_2:0n.37    -           0      37  SSD-NVM unassigned   -          -
node_B_2:0n.38    -           0      38  SSD-NVM unassigned   -          -
node_B_2:0n.39    -           0      39  SSD-NVM unassigned   -          -
node_B_2:0n.40    -           0      40  SSD-NVM unassigned   -          -
node_B_2:0n.41    -           0      41  SSD-NVM unassigned   -          -
node_B_2:0n.42    -           0      42  SSD-NVM unassigned   -          -
node_B_2:0n.43    -           0      43  SSD-NVM unassigned   -          -
32 entries were displayed.

cluster_B::>
```

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.

Related information

Cluster and SVM peering express configuration

Considerations when using dedicated ports

Considerations when sharing data ports

Configuring intercluster LIFs for cluster peering

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.

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.

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

```
cluster01::> network port show
                                                             Speed
(Mbps)
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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

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.

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

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

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`*

   The following example assigns ports "e0e" and" e0f" to failover group "intercluster01" on system "SVMcluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verify that the failover group was created:

   `network interface failover-groups show`

   For complete command syntax, see the man page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

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

ONTAP version	**Command**

9.6 and later	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`* `-failover -group` *`failover_group`*
9.5 and earlier	`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.

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

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-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 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs "cluster01_icl01", and "cluster01_icl02" on the "SVMe0e" port will fail over to the "e0f" port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Related information

Considerations when using dedicated ports

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.

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

```
cluster01::> network port show
                                                             Speed
(Mbps)
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:

In ONTAP 9.6 and later:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 and earlier:
`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.

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

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

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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:

In ONTAP 9.6 and later:

`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

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

```
cluster01::> network interface show -service-policy default-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 information

Considerations when sharing data ports

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.

About this task

- 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.

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.

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

```
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 the 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.

   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":

```
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`

```
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`

```
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
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

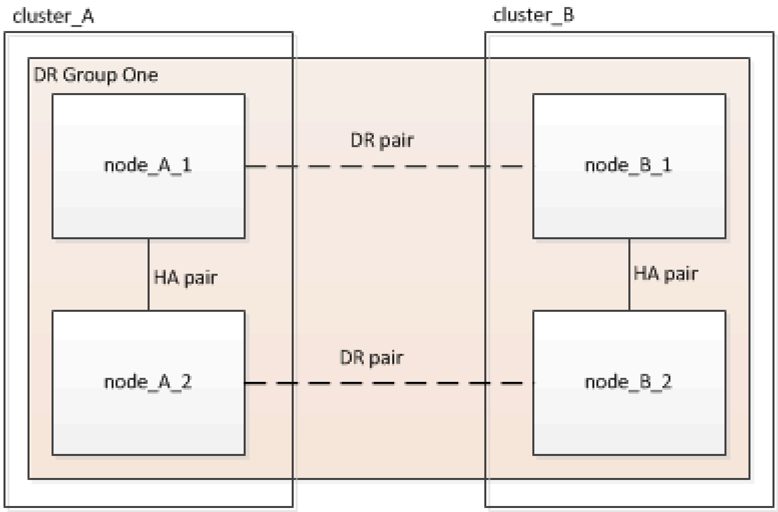
Creating the DR group

You must create the disaster recovery (DR) group relationships between the clusters.

About this task

You perform this procedure on one of the clusters in the MetroCluster configuration to create the DR relationships between the nodes in both clusters.

> The DR relationships cannot be changed after the DR groups are created.



Steps

1. Verify that the nodes are ready for creation of the DR group by entering the following command on each node:

   `metrocluster configuration-settings show-status`

   The command output should show that the nodes are ready:

```
cluster_A::> metrocluster configuration-settings show-status
Cluster                    Node          Configuration Settings Status
-------------------------- -------------
--------------------------------
cluster_A                  node_A_1      ready for DR group create
                           node_A_2      ready for DR group create
2 entries were displayed.
```

```
cluster_B::> metrocluster configuration-settings show-status
Cluster                    Node          Configuration Settings Status
-------------------------- -------------
--------------------------------
cluster_B                  node_B_1      ready for DR group create
                           node_B_2      ready for DR group create
2 entries were displayed.
```

2. Create the DR group:

   `metrocluster configuration-settings dr-group create -partner-cluster` *`partner-`*

cluster-name -local-node *local-node-name* -remote-node *remote-node-name*

This command is issued only once. It does not need to be repeated on the partner cluster. In the command, you specify the name of the remote cluster and the name of one local node and one node on the partner cluster.

The two nodes you specify are configured as DR partners and the other two nodes (which are not specified in the command) are configured as the second DR pair in the DR group. These relationships cannot be changed after you enter this command.

The following command creates these DR pairs:

- node_A_1 and node_B_1
- node_A_2 and node_B_2

```
Cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1
[Job 27] Job succeeded: DR Group Create is successful.
```

Configuring and connecting the MetroCluster IP interfaces

You must configure the MetroCluster IP interfaces that are used for replication of each node's storage and nonvolatile cache. You then establish the connections using the MetroCluster IP interfaces. This creates iSCSI connections for storage replication.

About this task

> You must choose the MetroCluster IP addresses carefully because you cannot change them after initial configuration.

- You must create two interfaces for each node. The interfaces must be associated with the VLANs defined in the MetroCluster RCF file.
- You must create all MetroCluster IP interface "A" ports in the same VLAN and all MetroCluster IP interface "B" ports in the other VLAN. Refer to Considerations for MetroCluster IP configuration.

+

> - Starting with ONTAP 9.8, certain platforms use a VLAN for the MetroCluster IP interface. By default, each of the two ports use a different VLAN: 10 and 20. You can also specify a different (non-default) VLAN higher than 100 (between 101 and 4095) using the `-vlan-id parameter` in the `metrocluster configuration-settings interface create` command.
> - Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.

+ The following platform models use VLANs and allow configuration of a non-default VLAN ID.

+

AFF platforms	FAS platforms
• AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

The following IP addresses and subnets are used in the examples:

Node	Interface	IP address	Subnet
node_A_1	MetroCluster IP interface 1	10.1.1.1	10.1.1/24
	MetroCluster IP interface 2	10.1.2.1	10.1.2/24
node_A_2	MetroCluster IP interface 1	10.1.1.2	10.1.1/24
	MetroCluster IP interface 2	10.1.2.2	10.1.2/24
node_B_1	MetroCluster IP interface 1	10.1.1.3	10.1.1/24
	MetroCluster IP interface 2	10.1.2.3	10.1.2/24
node_B_2	MetroCluster IP interface 1	10.1.1.4	10.1.1/24
	MetroCluster IP interface 2	10.1.2.4	10.1.2/24

The physical ports used by the MetroCluster IP interfaces depends on the platform model, as shown in the following table.

Platform model	MetroCluster IP port	VLAN ID	

AFF A800	e0b	Not used	
	e1b		
AFF A700 and FAS9000	e5a		
	e5b		
AFF A400	e3a		
	e3b		
AFF A320	e0g		
	e0h		
AFF A300 and FAS8200	e1a		
	e1b		
AFF A220 and FAS2750	e0a	10	On these systems, these physical ports are also used as cluster interfaces.
	e0b	20	
AFF A250 and FAS500f	e0c	10	
	e0d	20	
FAS8300 and FAS8700	e0c		
	e0d		

The port usage in the following examples is for an AFF A700 or a FAS9000 system.

Steps

1. Confirm that each node has disk automatic assignment enabled:

   `storage disk option show`

   Disk automatic assignment will assign pool 0 and pool 1 disks on a shelf-by-shelf basis.

   The Auto Assign column indicates whether disk automatic assignment is enabled.

```
Node         BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on          on           on            default
node_A_2             on          on           on            default
2 entries were displayed.
```

2. Verify you can create MetroCluster IP interfaces on the nodes:

   `metrocluster configuration-settings show-status`

   All nodes should be ready:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for interface create
              node_A_2     ready for interface create
cluster_B
              node_B_1     ready for interface create
              node_B_2     ready for interface create
4 entries were displayed.
```

3. Create the interfaces on node_A_1.

   - The port usage in the following examples is for an AFF A700 or a FAS9000 system (e5a and e5b). You must configure the interfaces on the correct ports for your platform model, as given above.
   - Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.
   - On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan-id` parameter if you don't want to use the default VLAN IDs.

   a. Configure the interface on port "e5a" on "node_A_1":

      `metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

      The following example shows the creation of the interface on port "e5a" on "node_A_1" with IP address "10.1.1.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
10.1.1.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

b. Configure the interface on port "e5b" on "node_A_1":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5b -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5b" on "node_A_1" with IP address "10.1.2.1":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

> You can verify that these interfaces are present using the `metrocluster configuration-settings interface show` command.

4. Create the interfaces on node_A_2.

> - The port usage in the following examples is for an AFF A700 or a FAS9000 system (e5a and e5b). You must configure the interfaces on the correct ports for your platform model, as given above.
> - Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.
> - On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan-id` parameter if you don't want to use the default VLAN IDs.

a. Configure the interface on port "e5a" on "node_A_2":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5a" on "node_A_2" with IP address "10.1.1.2":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e5a -address
10.1.1.2 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan -id` parameter if you don't want to use the default VLAN IDs. The following example shows the command for an AFF A220 system with a VLAN ID of 120:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

b. Configure the interface on port "e5b" on "node_A_2":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5b -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5b" on "node_A_2" with IP address "10.1.2.2":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e5b -address
10.1.2.2 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan -id` parameter if you don't want to use the default VLAN IDs. The following example shows the command for an AFF A220 system with a VLAN ID of 220:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0b -address
10.1.2.2 -netmask 255.255.255.0 -vlan-id 220
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

5. Create the interfaces on "node_B_1".

- The port usage in the following examples is for an AFF A700 or a FAS9000 system (e5a and e5b). You must configure the interfaces on the correct ports for your platform model, as given above.
- Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.
- On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan-id` parameter if you don't want to use the default VLAN IDs.

a. Configure the interface on port "e5a" on "node_B_1":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5a" on "node_B_1" with IP address "10.1.1.3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_B_1 -home-port e5a -address
10.1.1.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Configure the interface on port "e5b" on "node_B_1":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5b" on "node_B_1" with IP address "10.1.2.3":

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_B_1 -home-port e5b -address
10.1.2.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

6. Create the interfaces on "node_B_2".

- The port usage in the following examples is for an AFF A700 or a FAS9000 system (e5a and e5b). You must configure the interfaces on the correct ports for your platform model, as given above.
- Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.
- On platform models that support VLANs for the MetroCluster IP interface, you can include the `-vlan-id` parameter if you don't want to use the default VLAN IDs.

a. Configure the interface on port e5a on node_B_2:

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5a -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5a" on "node_B_2" with IP address "10.1.1.4":

```
cluster_B::>metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address
10.1.1.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Configure the interface on port "e5b" on "node_B_2":

`metrocluster configuration-settings interface create -cluster-name` *`cluster-name`* `-home-node` *`node-name`* `-home-port e5b -address` *`ip-address`* `-netmask` *`netmask`*

The following example shows the creation of the interface on port "e5b" on "node_B_2" with IP address "10.1.2.4":

```
cluster_B::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address
10.1.2.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

7. Verify that the interfaces have been configured:

`metrocluster configuration-settings interface show`

The following example shows that the configuration state for each interface is completed.

```
cluster_A::> metrocluster configuration-settings interface show
DR                                                               Config
Group Cluster Node    Network Address Netmask         Gateway   State
----- ------- ------- --------------- --------------- ---------
----------
1     cluster_A  node_A_1
                 Home Port: e5a
                      10.1.1.1     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.1     255.255.255.0   -         completed
                 node_A_2
                 Home Port: e5a
                      10.1.1.2     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.2     255.255.255.0   -         completed
      cluster_B  node_B_1
                 Home Port: e5a
                      10.1.1.3     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.3     255.255.255.0   -         completed
                 node_B_2
                 Home Port: e5a
                      10.1.1.4     255.255.255.0   -         completed
                 Home Port: e5b
                      10.1.2.4     255.255.255.0   -         completed
8 entries were displayed.
cluster_A::>
```

8. Verify that the nodes are ready to connect the MetroCluster interfaces:

   `metrocluster configuration-settings show-status`

   The following example shows all nodes in the "ready for connection" state:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for connection connect
              node_A_2     ready for connection connect
cluster_B
              node_B_1     ready for connection connect
              node_B_2     ready for connection connect
4 entries were displayed.
```

9. Establish the connections: `metrocluster configuration-settings connection connect`

   The IP addresses cannot be changed after you issue this command.

   The following example shows cluster_A is successfully connected:

```
cluster_A::> metrocluster configuration-settings connection connect
[Job 53] Job succeeded: Connect is successful.
cluster_A::>
```

10. Verify that the connections have been established:

    `metrocluster configuration-settings show-status`

    The configuration settings status for all nodes should be completed:

```
Cluster        Node          Configuration Settings Status
----------     -----------   ---------------------------------
cluster_A
               node_A_1      completed
               node_A_2      completed
cluster_B
               node_B_1      completed
               node_B_2      completed
4 entries were displayed.
```

11. Verify that the iSCSI connections have been established:

    a. 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. Display the connections:

       `storage iscsi-initiator show`

       On systems running ONTAP 9.5, there are eight MetroCluster IP initiators on each cluster that should appear in the output.

       On systems running ONTAP 9.4 and earlier, there are four MetroCluster IP initiators on each cluster that should appear in the output.

       The following example shows the eight MetroCluster IP initiators on a cluster running ONTAP 9.5:

```
cluster_A::*> storage iscsi-initiator show
```

```
Node Type Label    Target Portal          Target Name
Admin/Op
---- ---- -------- ------------------
------------------------------- --------

cluster_A-01
     dr_auxiliary
              mccip-aux-a-initiator
                   10.227.16.113:65200     prod506.com.company:abab44
up/up
              mccip-aux-a-initiator2
                   10.227.16.113:65200     prod507.com.company:abab44
up/up
              mccip-aux-b-initiator
                   10.227.95.166:65200     prod506.com.company:abab44
up/up
              mccip-aux-b-initiator2
                   10.227.95.166:65200     prod507.com.company:abab44
up/up
     dr_partner
              mccip-pri-a-initiator
                   10.227.16.112:65200     prod506.com.company:cdcd88
up/up
              mccip-pri-a-initiator2
                   10.227.16.112:65200     prod507.com.company:cdcd88
up/up
              mccip-pri-b-initiator
                   10.227.95.165:65200     prod506.com.company:cdcd88
up/up
              mccip-pri-b-initiator2
                   10.227.95.165:65200     prod507.com.company:cdcd88
up/up
cluster_A-02
     dr_auxiliary
              mccip-aux-a-initiator
                   10.227.16.112:65200     prod506.com.company:cdcd88
up/up
              mccip-aux-a-initiator2
                   10.227.16.112:65200     prod507.com.company:cdcd88
up/up
              mccip-aux-b-initiator
                   10.227.95.165:65200     prod506.com.company:cdcd88
up/up
              mccip-aux-b-initiator2
                   10.227.95.165:65200     prod507.com.company:cdcd88
up/up
```

```
      dr_partner
                  mccip-pri-a-initiator
                       10.227.16.113:65200     prod506.com.company:abab44
up/up
                  mccip-pri-a-initiator2
                       10.227.16.113:65200     prod507.com.company:abab44
up/up
                  mccip-pri-b-initiator
                       10.227.95.166:65200     prod506.com.company:abab44
up/up
                  mccip-pri-b-initiator2
                       10.227.95.166:65200     prod507.com.company:abab44
up/up
16 entries were displayed.
```

c. Return to the admin privilege level:

`set -privilege admin`

12. Verify that the nodes are ready for final implementation of the MetroCluster configuration:

`metrocluster node show`

```
cluster_A::> metrocluster node show
DR                                 Configuration  DR
Group Cluster Node                 State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_A
              node_A_1           ready to configure -     -
              node_A_2           ready to configure -     -
2 entries were displayed.
cluster_A::>
```

```
cluster_B::> metrocluster node show
DR                                 Configuration  DR
Group Cluster Node                 State          Mirroring Mode
----- ------- ------------------ -------------- --------- ----
-     cluster_B
              node_B_1           ready to configure -     -
              node_B_2           ready to configure -     -
2 entries were displayed.
cluster_B::>
```

Verifying or manually performing pool 1 drives assignment

Depending on the storage configuration, you must either verify pool 1 drive assignment or manually assign drives to pool 1 for each node in the MetroCluster IP configuration. The procedure you use depends on the version of ONTAP you are using.

Configuration type	Procedure
The systems meet the requirements for automatic drive assignment or, if running ONTAP 9.3, were received from the factory.	Verifying disk assignment for pool 1 disks
The configuration includes either three shelves, or, if it contains more than four shelves, has an uneven multiple of four shelves (for example, seven shelves), and is running ONTAP 9.5.	Manually assigning drives for pool 1 (ONTAP 9.4 or later)
The configuration does not include four storage shelves per site and is running ONTAP 9.4	Manually assigning drives for pool 1 (ONTAP 9.4 or later)
The systems were not received from the factory and are running ONTAP 9.3Systems received from the factory are pre-configured with assigned drives.	Manually assigning disks for pool 1 (ONTAP 9.3)

Verifying disk assignment for pool 1 disks

You must verify that the remote disks are visible to the nodes and have been assigned correctly.

Before you begin

You must wait at least ten minutes for disk auto-assignment to complete after the MetroCluster IP interfaces and connections were created with the `metrocluster configuration-settings connection connect` command.

Command output will show disk names in the form: node-name:0m.i1.0L1

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Steps

1. Verify pool 1 disks are auto-assigned:

   `disk show`

   The following output shows the output for an AFF A800 system with no external shelves.

   Drive autoassignment has assigned one quarter (8 drives) to "node_A_1" and one quarter to "node_A_2". The remaining drives will be remote (pool 1) disks for "node_B_1" and "node_B_2".

```
cluster_B::> disk show -host-adapter 0m -owner node_B_2
                        Usable     Disk              Container    Container
Disk                    Size       Shelf Bay Type    Type         Name
Owner
```

```
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_B_2:0m.i0.2L4  894.0GB    0     29  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.2L10 894.0GB    0     25  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L3  894.0GB    0     28  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L9  894.0GB    0     24  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L11 894.0GB    0     26  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L12 894.0GB    0     27  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L15 894.0GB    0     30  SSD-NVM shared      -
node_B_2
node_B_2:0m.i0.3L16 894.0GB    0     31  SSD-NVM shared      -
node_B_2
8 entries were displayed.

cluster_B::> disk show -host-adapter 0m -owner node_B_1
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i2.3L19 1.75TB     0     42  SSD-NVM shared      -
node_B_1
node_B_1:0m.i2.3L20 1.75TB     0     43  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L23 1.75TB     0     40  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L24 1.75TB     0     41  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L29 1.75TB     0     36  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L30 1.75TB     0     37  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L31 1.75TB     0     38  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L32 1.75TB     0     39  SSD-NVM shared       -
node_B_1
8 entries were displayed.

cluster_B::> disk show
                    Usable     Disk              Container   Container
```

```
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i1.0L6  1.75TB     0     1   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L8  1.75TB     0     3   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L17 1.75TB     0     18  SSD-NVM shared      -
node_A_1
node_B_1:0m.i1.0L22 1.75TB     0     17 SSD-NVM shared - node_A_1
node_B_1:0m.i1.0L25 1.75TB     0     12 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L2  1.75TB     0     5 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L7  1.75TB     0     2 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L14 1.75TB     0     7 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L21 1.75TB     0     16 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L27 1.75TB     0     14 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L28 1.75TB     0     15 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L1  1.75TB     0     4 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L5  1.75TB     0     0 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L13 1.75TB     0     6 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L18 1.75TB     0     19 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L26 1.75TB     0     13 SSD-NVM shared - node_A_1
node_B_1:0m.i2.3L19 1.75TB     0 42 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L20 1.75TB     0 43 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L23 1.75TB     0 40 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L24 1.75TB     0 41 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L29 1.75TB     0 36 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L30 1.75TB     0 37 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L31 1.75TB     0 38 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L32 1.75TB     0 39 SSD-NVM shared - node_B_1
node_B_1:0n.12      1.75TB     0 12 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.13      1.75TB     0 13 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.14      1.75TB     0 14 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.15      1.75TB 0 15 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.16      1.75TB 0 16 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.17      1.75TB 0 17 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.18      1.75TB 0 18 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.19      1.75TB 0 19 SSD-NVM shared - node_B_1
node_B_1:0n.24      894.0GB 0 24 SSD-NVM shared - node_A_2
node_B_1:0n.25      894.0GB 0 25 SSD-NVM shared - node_A_2
node_B_1:0n.26      894.0GB 0 26 SSD-NVM shared - node_A_2
node_B_1:0n.27      894.0GB 0 27 SSD-NVM shared - node_A_2
node_B_1:0n.28      894.0GB 0 28 SSD-NVM shared - node_A_2
node_B_1:0n.29      894.0GB 0 29 SSD-NVM shared - node_A_2
node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
```

```
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4  894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3  894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9  894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0       1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

cluster_B::>


cluster_A::> disk show
Usable Disk Container Container
Disk Size Shelf Bay Type Type Name Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
```

```
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
```

```
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>
```

Manually assigning drives for pool 1 (ONTAP 9.4 or later)

If the system was not preconfigured at the factory and does not meet the requirements for automatic drive assignment, you must manually assign the remote pool 1 drives.

About this task

This procedure applies to configurations running ONTAP 9.4 or later.

Details for determining whether your system requires manual disk assignment are included in Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later.

When the configuration includes only two external shelves per site, pool 1 drives for each site should be shared from the same shelf as shown in the following examples:

- node_A_1 is assigned drives in bays 0-11 on site_B-shelf_2 (remote)
- node_A_2 is assigned drives in bays 12-23 on site_B-shelf_2 (remote)

Steps

1. From each node in the MetroCluster IP configuration, assign remote drives to pool 1.
   a. Display the list of unassigned drives:

      ```
      disk show -host-adapter 0m -container-type unassigned
      ```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Assign ownership of remote drives (0m) to pool 1 of the first node (for example, node_A_1):

`disk assign -disk` *`disk-id`* `-pool 1 -owner` *`owner-node-name`*

`disk-id` must identify a drive on a remote shelf of `owner-node-name`.

c. Confirm that the drives were assigned to pool 1:

`disk show -host-adapter 0m -container-type unassigned`

The iSCSI connection used to access the remote drives appears as device 0m.

The following output shows that the drives on shelf 23 were assigned because they no longer appear in the list of unassigned drives:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

d. Repeat these steps to assign pool 1 drives to the second node on site A (for example, "node_A_2").

e. Repeat these steps on site B.

Manually assigning disks for pool 1 (ONTAP 9.3)

If you have at least two disk shelves for each node, you use ONTAP's auto-assignment functionality to automatically assign the remote (pool1) disks.

Before you begin

You must first assign a disk on the shelf to pool 1. ONTAP then automatically assigns the rest of the disks on the shelf to the same pool.

About this task

This procedure applies to configurations running ONTAP 9.3.

This procedure can be used only if you have at least two disk shelves for each node, which allows shelf-level auto-assignment of disks.

If you cannot use shelf-level auto-assignment, you must manually assign your remote disks so that each node has a remote pool of disks (pool 1).

The ONTAP automatic disk assignment feature assigns the disks on a shelf-by-shelf basis. For example:

- All the disks on site_B-shelf_2 are auto-assigned to pool1 of node_A_1
- All the disks on site_B-shelf_4 are auto-assigned to pool1 of node_A_2
- All the disks on site_A-shelf_2 are auto-assigned to pool1 of node_B_1
- All the disks on site_A-shelf_4 are auto-assigned to pool1 of node_B_2

You must "seed" the auto-assignment by specifying a single disk on each shelf.

Steps

1. From each node in the MetroCluster IP configuration, assign a remote disk to pool 1.

a. Display the list of unassigned disks:

`disk show -host-adapter 0m -container-type unassigned`

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Select a remote disk (0m) and assign ownership of the disk to pool 1 of the first node (for example, "node_A_1"):

`disk assign -disk` *`disk-id`* `-pool 1 -owner` *`owner-node-name`*

The `disk-id` must identify a disk on a remote shelf of `owner-node-name`.

The ONTAP disk auto-assignment feature assigns all disks on the remote shelf that contains the specified disk.

c. After waiting at least 60 seconds for disk auto-assignment to take place, verify that the remote disks on the shelf were auto-assigned to pool 1:

`disk show -host-adapter 0m -container-type unassigned`

> The iSCSI connection used to access the remote disks appears as device 0m.

The following output shows that the disks on shelf 23 have now been assigned and no longer appear:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
node_A_2:0m.i1.2L72       -    21  23 SSD     unassigned  -         -
node_A_2:0m.i1.2L74       -    21   1 SSD     unassigned  -         -
node_A_2:0m.i1.2L83       -    21  22 SSD     unassigned  -         -
node_A_2:0m.i1.2L90       -    21   7 SSD     unassigned  -         -
node_A_2:0m.i1.3L52       -    21   6 SSD     unassigned  -         -
node_A_2:0m.i1.3L59       -    21  13 SSD     unassigned  -         -
node_A_2:0m.i1.3L66       -    21  17 SSD     unassigned  -         -
node_A_2:0m.i1.3L73       -    21  12 SSD     unassigned  -         -
node_A_2:0m.i1.3L80       -    21   5 SSD     unassigned  -         -
node_A_2:0m.i1.3L81       -    21   2 SSD     unassigned  -         -
node_A_2:0m.i1.3L82       -    21  16 SSD     unassigned  -         -
node_A_2:0m.i1.3L91       -    21   3 SSD     unassigned  -         -
node_A_2:0m.i2.0L49       -    21  15 SSD     unassigned  -         -
node_A_2:0m.i2.0L50       -    21   4 SSD     unassigned  -         -
node_A_2:0m.i2.1L57       -    21  18 SSD     unassigned  -         -
node_A_2:0m.i2.1L58       -    21  11 SSD     unassigned  -         -
node_A_2:0m.i2.1L59       -    21  21 SSD     unassigned  -         -
node_A_2:0m.i2.1L65       -    21  20 SSD     unassigned  -         -
node_A_2:0m.i2.1L72       -    21   9 SSD     unassigned  -         -
node_A_2:0m.i2.1L80       -    21   0 SSD     unassigned  -         -
node_A_2:0m.i2.1L88       -    21   8 SSD     unassigned  -         -
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

d. Repeat these steps to assign pool 1 disks to the second node on site A (for example, "node_A_2").

e. Repeat these steps on site B.

Enabling automatic drive assignment in ONTAP 9.4

About this task

In ONTAP 9.4, if you disabled automatic drive assignment as directed previously in this procedure, you must reenable it on all nodes.

Considerations for automatic drive assignment and ADP systems in ONTAP 9.4 and later

Steps

1. Enable automatic drive assignment:

   `storage disk option modify -node node_name -autoassign on`

   You must issue this command on all nodes in the MetroCluster IP configuration.

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`

> 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`

   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

Creating a mirrored data aggregate on each node

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

About this task

- You should know what drives 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.
- Drives 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.

  In systems using ADP, aggregates are created using partitions in which each drive is partitioned in to P1, P2 and P3 partitions.

- 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:

   `storage aggregate create -mirror true`

   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 that are to be added to the aggregate
   - Number of drives to include

     > 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 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.

   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
```

Implementing the MetroCluster configuration

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

About this task

- There should be at least two non-root mirrored data aggregates on each cluster.

  You can verify this with the `storage aggregate show` command.

  > If you want to use a single mirrored data aggregate, then see Step 1 for instructions.

- The ha-config state of the controllers and chassis must be "mccip".

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.

The `metrocluster configure` command automatically pairs the two nodes with the lowest system IDs in each of the two clusters as disaster recovery (DR) partners. In a four-node MetroCluster configuration, there are two DR partner pairs. The second DR pair is created from the two nodes with higher system IDs.

Steps

1. Configure the MetroCluster in the following format:

If your MetroCluster configuration has…	Then do this…
Multiple data aggregates	From any node's prompt, configure MetroCluster: `metrocluster configure node-name`

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`

> 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":

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

[Job 121] Job succeeded: Configure is successful.
```

2. Verify the networking status on site A:

   `network port show`

   The following example shows the network port usage on a four-node MetroCluster configuration:

```
cluster_A::> network port show
                                                           Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verify the MetroCluster configuration from both sites in the MetroCluster configuration.
   a. Verify the configuration from site A:

      `metrocluster show`

```
cluster_A::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
Remote: cluster_B         Configuration state configured
                          Mode                normal
```

   b. Verify the configuration from site B:

      `metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

4. To avoid possible issues with nonvolatile memory mirroring, reboot each of the four nodes:

   `node reboot -node node-name -inhibit-takeover true`

5. Issue the `metrocluster show` command on both clusters to again verify the configuration.

Configuring the second DR group in an eight-node configuration

Repeat the previous tasks to configure the nodes in the second DR group.

Creating unmirrored data aggregates

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

About this task

- 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.

> In MetroCluster IP configurations, remote unmirrored aggregates are not accessible after a switchover

> 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. Enable unmirrored aggregate deployment:

   `metrocluster modify -enable-unmirrored-aggr-deployment true`

2. Verify that disk autoassignment is disabled:

`disk option show`

3. Install and cable the disk shelves that will contain the unmirrored aggregates.

   You can use the procedures in the Installation and Setup documentation for your platform and disk shelves.

   AFF and FAS Documentation Center

4. Manually assign all disks on the new shelf to the appropriate node:

   `disk assign -disk disk-id -owner owner-node-name`

5. Create the aggregate:

   `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 must also ensure that you are only including drives on the unmirrored shelf to the aggregate.

   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.

     The following command creates a unmirrored aggregate with 10 disks:

     ```
     controller_A_1::> storage aggregate create aggr1_controller_A_1
     -diskcount 10 -node controller_A_1
     [Job 15] Job is queued: Create aggr1_controller_A_1.
     [Job 15] The job is starting.
     [Job 15] Job succeeded: DONE
     ```

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

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

7. Disable unmirrored aggregate deployment:

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment false
   ```

8. Verify that disk autoassignment is enabled:

   ```
   disk option show
   ```

Related information

Disk and aggregate management

Checking the MetroCluster configuration

You can check that the components and relationships in the MetroCluster configuration are working correctly.

About this task

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.

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
   ```

   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: 9/13/2018 20:41:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
6 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.

   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

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
```

```
                                                    ownership-state
ok
                     controller_A_1_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_1_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok


controller_A_2       controller_A_2_aggr0
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_2_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                     controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

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

Cluster               Check                             Result
--------------------- ------------------------------- ---------
mccint-fas9000-0102
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
mccint-fas9000-0304
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
10 entries were displayed.
```

Related information

Disk and aggregate management

Network and LIF management

Completing ONTAP configuration

After configuring, enabling, and checking the MetroCluster configuration, you can proceed to complete the cluster configuration by adding additional SVMs, network interfaces and other ONTAP functionality as needed.

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

Configuring the MetroCluster Tiebreaker or ONTAP Mediator software

You can download and install on a third site either the MetroCluster Tiebreaker software, or, starting with ONTAP 9.7, the ONTAP Mediator.

Before you begin

You must have a Linux host available that has network connectivity to both clusters in the MetroCluster configuration. The specific requirements are in the MetroCluster Tiebreaker or ONTAP Mediator documentation.

If you are connecting to an existing Tiebreaker or ONTAP Mediator instance, you need the username, password, and IP address of the Tiebreaker or Mediator service.

If you must install a new instance of the ONTAP Mediator, follow the directions to install and configure the software.

Configuring the ONTAP Mediator service for unplanned automatic switchover

If you must install a new instance of the Tiebreaker software, follow the directions to install and configure the software.

MetroCluster Tiebreaker Software Installation and Configuration Guide

About this task

You cannot use both the MetroCluster Tiebreaker software and the ONTAP Mediator with the same MetroCluster configuration.

Considerations for using ONTAP Mediator or MetroCluster Tiebreaker

Step

1. Configure the ONTAP Mediator service or the Tiebreaker software:
   - If you are using an existing instance of the ONTAP Mediator, add the ONTAP Mediator service to ONTAP using the following command:

     ```
     metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
     ```

   - If you are using the Tiebreaker software, refer to the Tiebreaker 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*.

Configuring the ONTAP Mediator service for unplanned automatic switchover

Starting with ONTAP 9.7, the ONTAP Mediator service can assist the MetroCluster IP configuration in performing an automatic unplanned switchover by providing a physically separate repository for status information.

- The ONTAP Mediator service and MetroCluster Tiebreaker software should not both be used with the same MetroCluster configuration.
- The ONTAP Mediator service can support up to five MetroCluster configurations simultaneously.

Preparing to install the ONTAP Mediator service

Your environment must meet the following requirements. You may need to update your Linux version.

Network requirements for using Mediator in a MetroCluster configuration

To install the ONTAP Mediator service in a MetroCluster configuration, you must ensure that the configuration meets several network requirements.

- Round trip latency

  Round trip latency must be no more than 25 ms.

- MTU

  The MTU size must be at least 1400.

- Packet loss

  Packet loss must be less than or equal to 0.01%.

- Bandwidth

  The link between the Mediator service and the MetroCluster configuration must have at least 1 Gbps of bandwidth.

Firewall requirements for ONTAP Mediator

ONTAP Mediator uses a number of ports to communicate with specific services.

- If you are using a third-party firewall:
  - HTTPS access must be enabled.
  - It must be configured to allow access on ports 31784 and 3260.

    When using the default Red Hat or CentOS firewall, the firewall is automatically configured during Mediator installation.

The following table lists the ports that you must allow in your firewall:

Port/services	Source	Destination	Purpose
31784/tcp	ONTAP cluster management interfaces	ONTAP Mediator web server	REST API (HTTPS)

3260/tcp	ONTAP cluster	ONTAP Mediator iSCSI targets	iSCSI data connection for mailboxes

Guidelines for upgrading the ONTAP Mediator in a MetroCluster configuration

If you are upgrading the ONTAP Mediator you must meet the Linux version requirements and follow guidelines for the upgrade.

- The Mediator service can be upgraded from version 1.0 to 1.1.
- All Mediator versions are supported on MetroCluster IP configurations running ONTAP 9.7 or later.

Upgrading the host operating system and Mediator together

The following table provides the upgrade guidelines if you are upgrading from RHEL/CentOS 7.6 to a later RHEL/CentOS release in addition upgrading the Mediator version.

Target Linux version	Target Mediator version	Upgrade notes
RHEL/CentOS 7.7	1.1	• The upgrade must be performed in the following order: a. Upgrade the operating system from RHEL/CentOS version 7.6 to 7.7. **Note**: The ONTAP Mediator and Mediator-assisted automatic unplanned switchover is not available during the operating system upgrade. The Mediator is offline until the Mediator version 1.0 to 1.1 upgrade process is complete.. b. Reboot the host to apply the kernel module changes. c. Upgrade the Mediator from version 1.0 to 1.1. Installing or upgrading the ONTAP Mediator service • The storage iscsi-initiator show command will report that the connection to the Mediator service is down during the upgrade. • The ONTAP operating system will generate cf.mccip.med.auso.stDisabled EMS events during the upgrade. • The ONTAP operating system will generate a cf.mccip.med.auso.stEnabled EMS event when automatic unplanned switchover is re-enabled.

RHEL/CentOS 8.0 or 8.1	1.1	There is no direct upgrade path. You must remove the 1.0 version and install the 1.1 version after the operating system upgrade:
		1. Delete the Mediator service from the ONTAP configuration:
		`metrocluster configuration-settings mediator remove`
		2. Uninstall the 1.0 version of the Mediator service.
		Uninstalling the ONTAP Mediator service
		3. Upgrade the Linux operating system to version 8.0 or 8.1.
		4. Install the 1.1 version of the Mediator service.
		Installing or upgrading the ONTAP Mediator service
		5. Add the Mediator service to the ONTAP configuration:
		`metrocluster configuration-settings add -addressmediator-1.1-ip-address`

After the upgrade

After the Mediator and operating system upgrade is complete, you should issue the `storage iscsi-initiator show` command to confirm that the Mediator connections are up.

Reverting from a Mediator 1.1 installation

A direct revert from Mediator version 1.1 to 1.0 is not supported. You must remove the 1.1 version and reinstall the 1.0 version.

1. Delete the Mediator service from the ONTAP configuration:

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Uninstall the 1.1 version of the Mediator service.

   Uninstalling the ONTAP Mediator service

3. Install the 1.0 version of the Mediator service.

   Installing or upgrading the ONTAP Mediator service

4. Add the Mediator service to the ONTAP configuration:

   ```
   metrocluster configuration-settings add -addressmediator-1.0-ip-address
   ```

Recovering from Linux kernel upgrades

The ONTAP Mediator requires the SCST kernel module. If the Linux kernel is updated, this dependency may lead to a loss of service. It is highly recommended that you rebuild the SCST kernel module when any kernel package changes are made.

- Upgrading from ONTAP Mediator version 1.0 to 1.1 rebuilds the SCST module.
- Kernel module changes are applied after the Linux kernel is rebooted.

You can use either of the following procedures to recover from a kernel upgrade that has resulted in loss of service for the Mediator.

<table>
<tr><th>Procedure</th><th>Steps</th></tr>
<tr><td>Remove and reinstall the SCST kernel module</td><td>You must have the SCST tar bundle used by your version of Mediator:

• ONTAP Mediator 1.0 requires scst-3.3.0.tar.bz2
• ONTAP Mediator 1.1 requires scst-3.4.0.tar.bz2

1. Uninstall the SCST module:
a. Download and untar the SCST tar bundle required by your version of Mediator.
b. Run the following commands inside of the scst directory:

systemctl stop mediator-scst
make scstadm_uninstall
make iscsi_uninstall
make usr_uninstall
make scst_uninstall
depmod

2. Reinstall the SCST module for your version of Mediator by issuing the following commands inside of the scst directory:

make scst_install
make usr_install
make iscsi_install
make scstadm_install
depmod
patch /etc/init.d/scst <
/opt/netapp/lib/ontap_mediator/systemd/scst.
patch
reboot</td></tr>
</table>

Remove and reinstall ONTAP Mediator
 	
Note: This requires a reconfiguration of the Mediator in ONTAP.
	1. Delete the Mediator service from the ONTAP configuration:
	`metrocluster configuration-settings mediator remove`
	2. Uninstall the ONTAP Mediator service.
	3. Reinstall the Mediator service.
	4. Add the Mediator service to the ONTAP configuration:
	`metrocluster configuration-settings add -addressmediator-ip-address`

Installing or upgrading the ONTAP Mediator service

To install the ONTAP Mediator service, you must ensure all prerequisites are met, get the installation package and run the installer on the host.

Before you begin

You must meet the following prerequisites.

Mediator version	Supported Linux versions
1.3	Red Hat Enterprise Linux or CentOS 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3
1.2	Red Hat Enterprise Linux or CentOS 7.6, 7.7, 7.8, 8.0, 8.1

The kernel version must match the operating system version.

- 64-bit physical installation or virtual machine
- 8 GB RAM
- User: Root access

The best practices for installing Red Hat Enterprise Linux or CentOS and the associated repositories on your system are listed below. Systems installed or configured differently might require additional steps.

- You must install Red Hat Enterprise Linux or CentOS according to Red Hat best practices.
- While installing the ONTAP Mediator service on Red Hat Enterprise Linux or CentOS, the system must have access to the appropriate repository so that the installation program can access and install all the required software dependencies.
- For the yum installer to find dependent software in the Red Hat Enterprise Linux repositories, you must have registered the system during the Red Hat Enterprise Linux installation or afterwards by using a valid Red Hat subscription.

  See the Red Hat documentation for information about the Red Hat Subscription Manager.
- The following ports must be unused and available for the Mediator:
  - 31784

    ◦ 3260

* If using a third-party firewall: refer to Firewall requirements for ONTAP Mediator
* If the Linux host is in a location without access to the internet, you can either install the packages manually or you must ensure that the required packages are available in a local repository.

  You can use the following link for information about setting up a repository.

  If you are using Link Aggregation Control Protocol (LACP) in a Linux environment, you must correctly configure the kernel and make sure the `sysctl net.ipv4.conf.all.arp_ignore` is set to "2".

  The following packages are required by the ONTAP Mediator service:

All RHEL/CentOS versions	Additional packages for RHEL/CentOS 7.x	Additional packages for RHEL/CentOS 8.x
• openssl • openssl-devel • kernel-devel • gcc • libselinux-utils • make • redhat-lsb-core • patch • bzip2 • python36 • python36-devel • perl-Data-Dumper • perl-ExtUtils-MakeMaker • python3-pip	• policycoreutils-python • python36-pip	• elfutils-libelf-devel • policycoreutils-python-utils

* If signature verification is configured, it must be disabled. This can be done in one of two ways:
    ◦ If the UEFI SecureBoot mechanism is configured, disable it.
    ◦ Disable the signature verification mechanism by updating and regenerating the grub.cfg file:
        i. Open the /etc/default/grub file.
        ii. Add the string module.sig_enforce=0 to the end of the GRUB_CMDLINE_LINUX statement.
        iii. Regenerate the grub.cfg file to implement the change:

```
update-bootloader || update-grub || grub2-mkconfig -o
/boot/grub2/grub.cfg
```

        iv. Reboot the host.

The Mediator installation package is a self-extracting compressed tar file that includes:

* An RPM file containing all dependencies that cannot be obtained from the supported release's repository.
* An install script.

A valid SSL certification is recommended, as documented in this procedure.

This procedure is used for an installation or an upgrade of an existing installation.

Guidelines for upgrading the ONTAP Mediator in a MetroCluster configuration

Enable access to the repositories

If your operating system is…	You must provide access to these repositories…
RHEL 7.x	rhel-7-server-optional-rpms
CentOS 7.x	C7.6.1810 - Base repository
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
CentOS 8.0	kernel-devel

Enable access to the repositories listed above so Mediator can access the required packages during the installation process. Use the procedure below for your operating system.

* Procedure for RHEL 7.x operating system.
* Procedure for RHEL 8.x operating system.
* Procedure for CentOS 7.x operating system.
* Procedure for CentOS 8.0.1095 or later operating system.

Procedure for RHEL 7.x operating system

If your operating system is **RHEL 7.x**:

Steps

1. Subscribe to the required repository:

   ```
   subscription-manager repos --enable rhel-7-server-optional-rpms
   ```

   The following example shows the execution of this command:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-7-server-
   optional-rpms
   Repository 'rhel-7-server-optional-rpms' is enabled for this system.
   ```

2. Run the `yum repolist` command.

   The following example shows the execution of this command. The "rhel-7-server-optional-rpms" repository should appear in the list.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
|  26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                      repo name
status
rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise Linux 7
Server - Optional (RPMs)   19,447
rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise Linux 7
Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

Procedure for RHEL 8.x operating system

If your operating system is **RHEL 8.x**:

Steps

1. Subscribe to the required repository:

   `subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms`

   `subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms`

   The following example shows the execution of this command:

   ```
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-baseos-rpms
   [root@localhost ~]# subscription-manager repos --enable rhel-8-for-
   x86_64-appstream-rpms
   Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this system.
   Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
   system.
   ```

2. Run the `yum repolist` command.

   The newly subscribed repositories should appear in the list.

Procedure for CentOS 7.x operating system

If your operating system is **CentOS 7.x**:

Steps

1. Add the C7.6.1810 - Base repository. The C7.6.1810 - Base vault repository contains the kernel-devel package needed for ONTAP Mediator.
2. Add the following lines to /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$
basearch/gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Run the `yum repolist` command.

   The following example shows the execution of this command. The CentOS-7.6.1810 - Base repository should appear in the list.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                                   | 3.6
kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz                            | 166
kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db                          | 6.0
MB  00:00:04
repo id                                          repo name
status
C7.6.1810-base/x86_64                            CentOS-7.6.1810 - Base
10,019
base/7/x86_64                                    CentOS-7 - Base
10,097
extras/7/x86_64                                  CentOS-7 - Extras
307
updates/7/x86_64                                 CentOS-7 - Updates
1,010
repolist: 21,433
[root@localhost ~]#
```

Procedure for CentOS 8.0.1905 or later operating system

If your operating system is **CentOS 8.0.1905 or later builds**:

Before you begin

In the CentOS Vault, locate the kernel-devel package that matches your operating system. Because the latest versions of the 8.0 (CentOS 8.0.1905 and later) core reside in the CentOS Vault, you must provide access to the matching kernel-devel package to compile the needed kernel module.

Steps

1. Issue the following command to directly install the kernel-devel package:

   ```
   rpm -i http://vault.centos.org/8.0.1905/BaseOS/x86_64/os/Packages/kernel-devel-$(uname -r).rpm
   ```

   > The above command is an example that is specific to CentOS 8.0.1905. Change the path where appropriate for other CentoOS 8.x builds.

2. If the system displays an error indicating that the package is already installed, remove the package and try again:

   a. Remove the kernel-devel package:

      ```
      yum remove kernel-devel
      ```

   b. Repeat the `rpm` command shown in Step 1.

Download the Mediator installation package

Steps

1. Download the Mediator installation package from the ONTAP Mediator page.

   ONTAP Mediator download page

2. Confirm that the Mediator installation package is in the target directory:

   ```
   ls
   ```

   ```
   [root@mediator-host ~]#ls
   ./ontap-mediator_1.3
   ```

   If you are at a location without access to the internet, you must ensure that the installer has access to the required packages.

3. If necessary, move the Mediator installation package from the download directory to the installation directory on the Linux Mediator host.

Install the ONTAP Mediator installation package

Step

1. Install the Mediator installation package and respond to the prompts as required:

```
./ontap-mediator_1.3
```

The installation process proceeds to create the required accounts and install required packages. If you have a previous version of Mediator installed on the host, you will be prompted to confirm that you want to upgrade.

Example of ONTAP Mediator installation (console output)

Verify the installation

Steps

1. Run the following command to view the status of the ONTAP Mediator services:

```
systemctl
```

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator mediator-scst

        · ontap_mediator.service - ONTAP Mediator
            Loaded: loaded
(/opt/netapp/lib/ontap_mediator/systemd/ontap_mediator.service; enabled;
vendor preset: disabled)

            Active: active (running) since Thu 2020-06-18 09:55:02 EDT;
3 days ago

         Main PID: 3559 (uwsgi)

            Status: "uWSGI is ready"

            CGroup: /system.slice/ontap_mediator.service

                    \u251c\u25003559
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

                    \u251c\u25004510
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

                    \u2514\u25004512
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini



         Jun 18 09:54:43 scspr1915530002 systemd[1]: Starting ONTAP
Mediator...
```

```
         Jun 18 09:54:45 scspr1915530002 ontap_mediator[3559]: [uWSGI]
getting INI configuration from
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

         Jun 18 09:55:02 scspr1915530002 systemd[1]: Started ONTAP
Mediator.



         · mediator-scst.service
            Loaded: loaded
(/opt/netapp/lib/ontap_mediator/systemd/mediator-scst.service; enabled;
vendor preset: disabled)

            Active: active (running) since Thu 2020-06-18 09:54:51 EDT;
3 days ago

           Process: 3564 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)

         Main PID: 4202 (iscsi-scstd)

            CGroup: /system.slice/mediator-scst.service

                    \u2514\u25004202 /usr/local/sbin/iscsi-scstd



         Jun 18 09:54:43 scspr1915530002 systemd[1]: Starting mediator-
scst.service...

         Jun 18 09:54:48 scspr1915530002 iscsi-scstd[4200]:
max_data_seg_len 1048576, max_queued_cmds 2048

         Jun 18 09:54:51 scspr1915530002 scst[3564]: Loading and
configuring SCST[  OK  ]

         Jun 18 09:54:51 scspr1915530002 systemd[1]: Started mediator-
scst.service.

         [root@scspr1915530002 ~]#
```

2. Confirm the ports the ONTAP Mediator service is using: netstat

```
        [root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

        tcp        0      0 0.0.0.0:31784           0.0.0.0:*
LISTEN

        tcp        0      0 0.0.0.0:3260            0.0.0.0:*
LISTEN

        tcp6       0      0 :::3260                 :::*
LISTEN
```

Result

The ONTAP Mediator service is now installed and running. Further configuration must be performed in the ONTAP storage system to use the Mediator features.

Configuring the ONTAP Mediator service from a MetroCluster IP configuration

The ONTAP Mediator service must be configured on the ONTAP node for use in a MetroCluster IP configuration.

Before you begin

- The ONTAP Mediator must have been successfully installed on a network location that can be reached by both MetroCluster sites.
- You must have the IP address of the host running the ONTAP Mediator service.
- You must have the username and password for the ONTAP Mediator service.
- All nodes of the MetroCluster IP configuration must be online.

About this task

- This task enables automatic unplanned switchover by default.
- This task can be performed on the ONTAP interface of any node in the MetroCluster IP configuration.
- A single installation of the ONTAP Mediator service can be configured with up to five MetroCluster IP configurations.

Steps

1. Add the ONTAP Mediator service to ONTAP using the following command:

   `metrocluster configuration-settings mediator add -mediator-address` *`ip-address-of-mediator-host`*

   > ⓘ You will be prompted for the username and password for the Mediator admin user account.

2. Verify that the automatic switchover feature in enabled:

   `metrocluster show`

3. Verify that the Mediator is now running.
   a. Show the Mediator virtual disks:

      `storage disk show -container-type mediator`

```
 cluster_A::> storage disk show -container-type mediator
                        Usable           Disk    Container
Container
 Disk                   Size Shelf Bay Type    Type        Name
Owner
 ---------------- ---------- ----- --- ------- ----------- ---------
--------
 NET-1.5                   -     -   - VMDISK  mediator    -
node_A_2
 NET-1.6                   -     -   - VMDISK  mediator    -
node_B_1
 NET-1.7                   -     -   - VMDISK  mediator    -
node_B_2
 NET-1.8                   -     -   - VMDISK  mediator    -
node_A_1
```

   b. Set the privilege mode to advanced:

      `set advanced`

```
 cluster_A::> set advanced
```

   c. Display the initiators labelled as mediator:

      `storage iscsi-initiator show -label mediator`

```
cluster_A::*> storage iscsi-initiator show -label mediator
   (storage iscsi-initiator show)
  +
Status
 Node Type Label    Target Portal      Target Name
Admin/Op
 ---- ---- -------- ------------------
-------------------------------- --------
 node_A_1
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68- 00a098cbca9e:1 up/up
 node_A_2
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68-00a098cbca9e:1 up/up
```

Connecting a MetroCluster configuration to a different ONTAP Mediator instance

If you want to connect the MetroCluster nodes to a different ONTAP Mediator instance, you must unconfigure and then reconfigure the Mediator connection in the ONTAP software.

Before you begin

You need the username, password, and IP address of the new ONTAP Mediator instance.

About this task

These commands can be issued from any node in the MetroCluster configuration.

Steps

1. Remove the current ONTAP Mediator from the MetroCluster configuration:

   `metrocluster configuration-settings mediator remove`

2. Establish the new ONTAP Mediator connection to the MetroCluster configuration:

   `metrocluster configuration-settings mediator add -mediator-address` *`ip-address-of-mediator-host`*

Changing the ONTAP Mediator password

After you have installed ONTAP Mediator service, you might want to change the password. You can change the password in two ways.

About this task

This task is performed on the Linux host on which the ONTAP Mediator service is installed.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

`/usr/local/bin/mediator_change_password`

Procedure

Change the password by choosing one of the following options:

- Run the mediator_change_password command and respond to the prompts as shown in the following example:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
             Old Password:
             New Password:
         Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- Run the following command:

  `MEDIATOR_USERNAME= mediatoradmin MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password`

  The example shows the password is changed from "mediator1" to "mediator2".

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

Changing the ONTAP Mediator user name

After you have installed ONTAP Mediator service, you might want to change the user name. You can change the password in two ways.

About this task

This task is performed on the Linux host on which the ONTAP Mediator service is installed.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

```
/usr/local/bin/mediator_username
```

Procedure

Change the username by choosing one of the following options:

- Run the command mediator_change_user and respond to the prompts as shown in the following example:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- Run the following command:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
 [root@mediator-host ~]# MEDIATOR_USERNAME= mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME= mediatoradmin
mediator_change_user
 The account username has been modified successfully.
 [root@mediator-host ~]#
```

Uninstall the ONTAP Mediator service

If necessary, you can remove the ONTAP Mediator service.

Before you begin

The Mediator must be disconnected from ONTAP before you remove the Mediator service.

About this task

This task is performed on the Linux host on which the ONTAP Mediator service is installed.

If you are unable to reach this command, you might need to run the command using the full path as shown in the following example:

```
/usr/local/bin/uninstall_ontap_mediator
```

Step

1. Uninstall the ONTAP Mediator service:

```
uninstall_ontap_mediator
```

```
[root@mediator-host ~]# uninstall_ontap_mediator

ONTAP Mediator: Self Extracting Uninstaller

+ Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
+ Remove successful.
[root@mediator-host ~]#
```

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 the command is issued from will switch over the partner site.

For MetroCluster IP configurations:

- For ONTAP 9.4 and earlier:
  - Mirrored aggregates will become degraded after the negotiated switchover.
- For ONTAP 9.5 and later:
  - Mirrored aggregates will remain in normal state if the remote storage is accessible.
  - Mirrored aggregates will become degraded after the negotiated switchover if access to the remote storage is lost.
- For ONTAP 9.8 and later:
  - Unmirrored aggregates that are located at the disaster site will become unavailable if access to the remote storage is lost. This might lead to a controller outage.

Steps

1. Confirm that all nodes are in the configured state and normal mode:

   `metrocluster node show`

```
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`

```
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`

```
cluster_A::>  metrocluster node show

Cluster                        Configuration State    Mode
------------------------------ ----------------------
------------------------
Local: cluster_A                configured             switchover
Remote: cluster_B               not-reachable          -
              configured             normal
```

4. Confirm that the switchover operation was successful:

   `metrocluster operation show`

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

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:

   `metrocluster heal aggregates`

   The following example shows the successful completion of the command:

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

2. If the system is running ONTAP 9.4 or earlier, heal the root aggregate:

   `metrocluster heal root-aggregates`

   This step is required on the following configurations:

   - MetroCluster FC configurations.
   - MetroCluster IP configurations running ONTAP 9.4 or earlier. The following example shows the successful completion of the command:

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

3. Verify that healing is completed:

   `metrocluster node show`

   The following example shows the successful completion of the command:

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   heal roots
completed
      cluster_B
              node_B_2         unreachable    -         switched over
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 -instance` commands to monitor the status of healing and determine the cause of a failure.

4. Verify that all aggregates are mirrored:

   `storage aggregate show`

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

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                              mirrored,
                                                              normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                              mirrored,
                                                              normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                              mirrored,
                                                              normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

5. Boot nodes from the disaster site.
6. Check the status of switchback recovery:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
             node_A_1            configured     enabled   heal roots
completed
      cluster_B
             node_B_2            configured     enabled   waiting for
switchback
                                                          recovery
2 entries were displayed.
```

7. Perform the switchback:

   `metrocluster switchback`

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

8. Confirm status of the nodes:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                                Configuration  DR
Group Cluster Node                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`

   The output should show a successful state.

```
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: -
```

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 PDUs are disconnected.
- No failover or loss of service should occur.

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:

   `system environment sensors show -state fault`

   `storage shelf show -errors`

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

Node Sensor              State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- --------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
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`

```
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`

```
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*
```

```
cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

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
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

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.

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

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 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)
                                                              Usable
Physical
     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)
                                                              Usable
Physical
     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)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                              Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   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`

   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,

mirror

degraded
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,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(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)
                                                              Usable
Physical
     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 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                              Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                        -   -          -  827.7GB
- (failed)
     parity   FAILED                        -   -          -  827.7GB
- (failed)
     data     FAILED                        -   -          -  827.7GB
- (failed)
     data     FAILED                        -   -          -  827.7GB
- (failed)
     data     FAILED                        -   -          -  827.7GB
- (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                              Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                       0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                       0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                       0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
      data     2.30.20                          0   BSAS    7200  827.7GB
828.0GB (normal)
      data     2.30.14                          0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

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*`

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

cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

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
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Physically power on the shelf.

   Resynchronization starts automatically.

9. Verify that resynchronization has started:

   `storage aggregate show`

   The affected aggregate should have a RAID status of "resyncing", 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`

    The affected aggregate should have a RAID status of "normal", as shown in the following 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,

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
```

Considerations when removing MetroCluster configurations

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.

> You cannot reverse the MetroCluster unconfiguration. This process should only be done with the assistance of technical support.

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.

The ONTAP configuration of the two clusters, including networking, should be identical, because the MetroCluster feature relies on the ability of a cluster to seemlessly serve data for its partner in the event of a switchover.

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.

MetroCluster operations in ONTAP System Manager

Depending on your ONTAP version, some MetroCluster-specific operations can be performed using ONTAP System Manager.

- Switchover and switchback in MetroCluster IP configurations (starting in ONTAP 9.7).
- Provision and grow of mirrored aggregates in the MetroCluster IP configurations (starting in ONTAP 9.8).

  Unmirrored aggregates are not supported in System Manager.

FlexCache support in a MetroCluster configuration

Starting with ONTAP 9.7, FlexCache volumes are supported on MetroCluster configurations. You should be aware of requirements for manual repeering after switchover or switchback operations.

SVM repeering after switchover when FlexCache origin and cache are within the same MetroCluster site

After a negotiated or unplanned switchover, any SVM FlexCache peering relationship within the cluster must be manually configured.

For example, SVMs vs1 (cache) and vs2 (origin) are on site_A. These SVMs are peered.

After switchover, SVMs vs1-mc and vs2-mc are activated at the partner site (site_B). They must be manually repeered for FlexCache to work using the vserver peer repeer command.

SVM repeering after switchover or switchback when a FlexCache destination is on a third cluster and in disconnected mode

For FlexCache relationships to a cluster outside of the MetroCluster configuration, the peering must always be manually reconfigured after a switchover if the involved clusters are in disconnected mode during switchover.

For example:

- One end of the FlexCache (cache_1 on vs1) resides on MetroCluster site_A has one end of the FlexCache
- The other end of the FlexCache (origin_1 on vs2) resides on site_C (not in the MetroCluster configuration)

When switchover is triggered, and if site_A and site_C are not connected, you must manually repeer the SVMs on site_B (the switchover cluster) and site_C using the vserver peer repeer command after the switchover.

When switchback is performed, you must again repeer the SVMs on site_A (the original cluster) and site_C.

Related information

FlexCache volumes management

FabricPool support in MetroCluster configurations

Starting with ONTAP 9.7, MetroCluster configurations support FabricPool storage tiers.

For general information on using FabricPools, see the *Disks and Aggregates Power Guide*.

Disk and aggregate management

Considerations when using FabricPools

- The clusters must have FabricPool licenses with matching capacity limits.
- The clusters must have IPSpaces with matching names.

  This can be the default IPSpace, or an IP space an administer has created. This IPSpace will be used for FabricPool object store configuration setups.

- For the selected IPSpace, each cluster must have an intercluster LIF defined that can reach the external object store

Configuring an aggregate for use in a mirrored FabricPool

> ⓘ Before you configure the aggregate you must set up object stores as described in "Setting up object stores for FabricPool in a MetroCluster configuration" in the *Disks and Aggregates Power Guide*.

Disk and aggregate management

To configure an aggregate for use in a FabricPool:

1. Create the aggregate or select an existing aggregate.
2. Mirror the aggregate as a typical mirrored aggregate within the MetroCluster configuration.
3. Create the FabricPool mirror with the aggregate, as described in the *Disks and Aggregates Power Guide*:

[Disk and aggregate management](#)

a. Attach a primary object store.

   This object store is physically closer to the cluster.

b. Add a mirror object store.

   This object store is physically further distant to the cluster than the primary object store.

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).

> 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

Network and LIF management

IPspace object replication and subnet configuration requirements

Requirements for LIF creation in a MetroCluster configuration

[LIF replication and placement requirements and issues]

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                     Broadcast                   Avail/
Name      Subnet           Domain    Gateway           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                     Broadcast                   Avail/
Name      Subnet           Domain    Gateway           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.

Related information

Requirements for LIF creation in a MetroCluster configuration

LIF replication and placement requirements and issues

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
- NFS and SAN configurations: You must use different storage virtual machines (SVMs) for both the unmirrored and mirrored aggregates

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.

Related information

IPspace object replication and subnet configuration requirements

LIF replication and placement requirements and 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:

Condition	LIF type: FC	LIF type: IP/iSCSI

Node identification	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.	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.
Port identification	ONTAP identifies the connected FC target ports on the DR cluster.	The ports on the DR cluster that are in the same IPspace as the source LIF are selected for a reachability check.If there are no ports in the DR cluster in the same IPspace, the LIF cannot be placed. All of the ports in the DR cluster that are already hosting a LIF in the same IPspace and subnet are automatically marked as reachable; and can be used for placement. These ports are not included in the reachability check.
Reachability check	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.	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.

Port selection	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.	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.
LIF placement	From the reachable ports, ONTAP selects the least loaded port for placement.	From the selected ports, ONTAP selects the least loaded port for placement.

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.

> 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.

Related information

IPspace object replication and subnet configuration requirements

Requirements for LIF creation in a MetroCluster configuration

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.

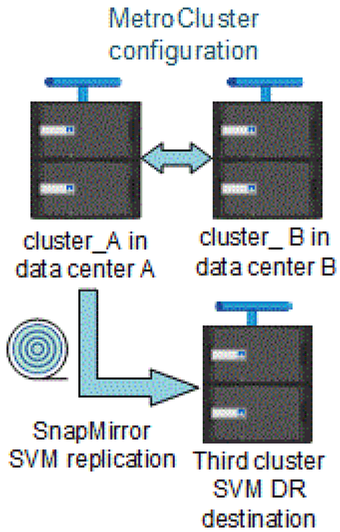
You should be aware of the following requirements and limitations of using SVMs with SnapMirror disaster recovery:

- 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.

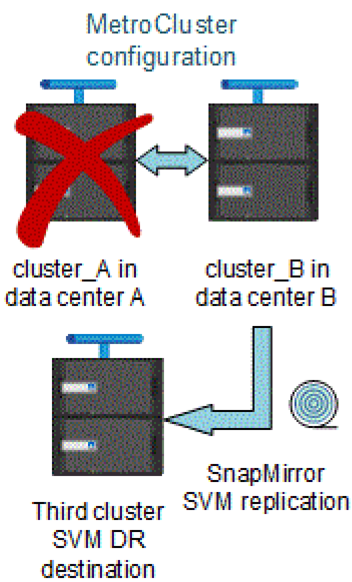
- When a MetroCluster configuration is in a steady state, the MetroCluster sync-destination SVM cannot be the source of an SVM disaster recovery relationship, since the volumes are not online.

  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:



- During the switchover and switchback processes, replication to the SVM DR destination might fail.

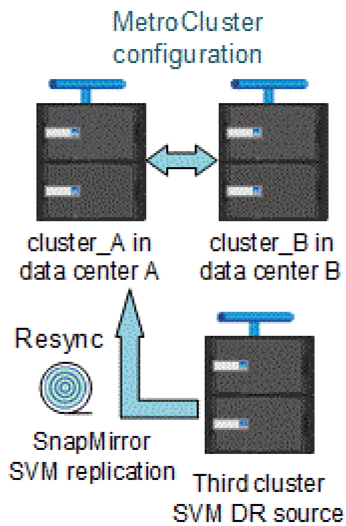
  However, after the switchover or switchback process completes, the next SVM DR scheduled updates will succeed.

See "Replicating the SVM configuration" in Data protection for details on configuring an SVM DR relationship.

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 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.

ⓘ 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.

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
```

Where to find additional information

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

MetroCluster and miscellaneous guides

Guide	Content
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
Stretch MetroCluster installation and configuration	• Stretch MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • Configuring the MetroCluster in ONTAP
MetroCluster management	• Understanding the MetroCluster configuration • Switchover, healing, and switchback
Disaster Recovery Guide	• Disaster recovery • Forced switchover • Recovery from a multi-controller or storage failure

MetroCluster Maintenance Guide	• Guidelines for maintenance in a MetroCluster FC configuration • Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches • Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster FC configuration • Expanding a two-node fabric-attached or stretch MetroCluster FC configuration to a four-node MetroCluster configuration. • Expanding a four-node fabric-attached or stretch MetroCluster FC configuration to an eight-node MetroCluster FC configuration.
MetroCluster Upgrade and Expansion Guide	• Upgrading or refreshing a MetroCluster configuration • Expanding a MetroCluster configuration by adding additional nodes
MetroCluster Transition Guide	• Transitioning from a MetroCluster FC configuration to a MetroCluster IP configuration
MetroCluster Upgrade, Transition, and Expansion Guide	• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software
AFF and FAS Documentation Center **Note:** The standard storage shelf maintenance procedures can be used with MetroCluster IP configurations.	• Hot-adding a disk shelf • Hot-removing a disk shelf
Copy-based transition	• Transitioning data from 7-Mode storage systems to clustered storage systems
ONTAP concepts	• How mirrored aggregates work

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.

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

Differences between ONTAP MetroCluster configurations

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

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

Feature	IP configurations	Fabric attached configurations		Stretch configurations	
		Four- or eight-node	**Two-node**	**Two-node bridge-attached**	**Two-node direct-attached**
Number of controllers	Four or eight*	Four or eight	Two	Two	Two
Uses an FC switch storage fabric	No	Yes	Yes	No	No
Uses an IP switch storage fabric	Yes	No	No	No	No
Uses FC-to-SAS bridges	No	Yes	Yes	Yes	No

Uses direct-attached SAS storage	Yes (local attached only)	No	No	No	Yes
Supports ADP	Yes (starting in ONTAP 9.4)	No	No	No	No
Supports local HA	Yes	Yes	No	No	No
Supports ONTAP AUSO	No	Yes	Yes	Yes	Yes
Supports unmirrored aggregates	Yes (starting in ONTAP 9.8)	Yes	Yes	Yes	Yes
Supports array LUNs	No	Yes	Yes	Yes	Yes
Supports ONTAP Mediator	Yes (starting in ONTAP 9.7)	No	No	No	No
Supports MetroCluster Tiebreaker	Yes (not in combination with ONTAP Mediator)	Yes	Yes	Yes	Yes
Supports All SAN Arrays	Yes	Yes	Yes	Yes	Yes

Important

Notice the following considerations for eight-node MetroCluster IP configurations:

- Eight-node configurations are supported starting in ONTAP 9.9.1.
- Only NetApp-validated MetroCluster switches (ordered from NetApp) are supported.
- Configurations using IP-routed (layer 3) backend connections are not supported.
- Configurations using shared private layer 2 networks are not supported.
- Configurations using a Cisco 9336C-FX2 shared switch are not supported.

Support for All SAN Array systems in MetroCluster configurations

Some of the All SAN Arrays (ASAs) are supported in MetroCluster configurations. In the MetroCluster documentation, the information for AFF models applies to the corresponding ASA system. For example, all cabling and other information for the AFF A400 system also applies to the ASA AFF A400 system.

Supported platform configurations are listed in the NetApp Hardware Universe.

Cluster peering

Each MetroCluster site is configured as a peer to its partner site. You must be familiar with the prerequisites and guidelines for configuring the peering relationships. This is important when deciding on 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 connectivity between 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 used in each cluster must meet the following requirements:

- The subnet must have enough IP addresses available to allocate to one intercluster LIF per node.

  For example, in a six-node cluster, the subnet used for intercluster communication must have six available IP addresses.

Each node must have an intercluster LIF with an IP address on the intercluster network.

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

> ONTAP 9 enables you to migrate your peering networks from IPv4 to IPv6 by optionally allowing both protocols to be present simultaneously on the intercluster LIFs. In earlier releases, all intercluster relationships for an entire cluster were either IPv4 or IPv6. This meant that changing protocols was a potentially disruptive event.

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 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 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
* Bidirectional HTTPS between the intercluster LIFs

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 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. This 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 the 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. This 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

Considerations when using unmirrored aggregates

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

Considerations for unmirrored aggregates when doing maintenance requiring power shutdown

If you are performing a 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 take any unmirrored aggregates offline, 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. This is the result of a power shutdown or a loss of ISLs.

Considerations for unmirrored aggregates and hierarchical namespaces

If you are 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 metadata volume and data SVM root volumes

The configuration replication service (CRS) metadata volume and data SVM root volumes must be on a mirrored aggregate. You cannot move these volumes to an unmirrored aggregate. If they are on an 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

SVMs 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.

Considerations for unmirrored aggregates and SAN

In ONTAP versions prior to 9.9.1, a LUN should not be located on an unmirrored aggregate. Configuring a LUN on an unmirrored aggregate can result in a switchover operation that exceeds 120 seconds and a data outage.

Firewall usage at MetroCluster sites

Considerations for firewall usage at MetroCluster sites

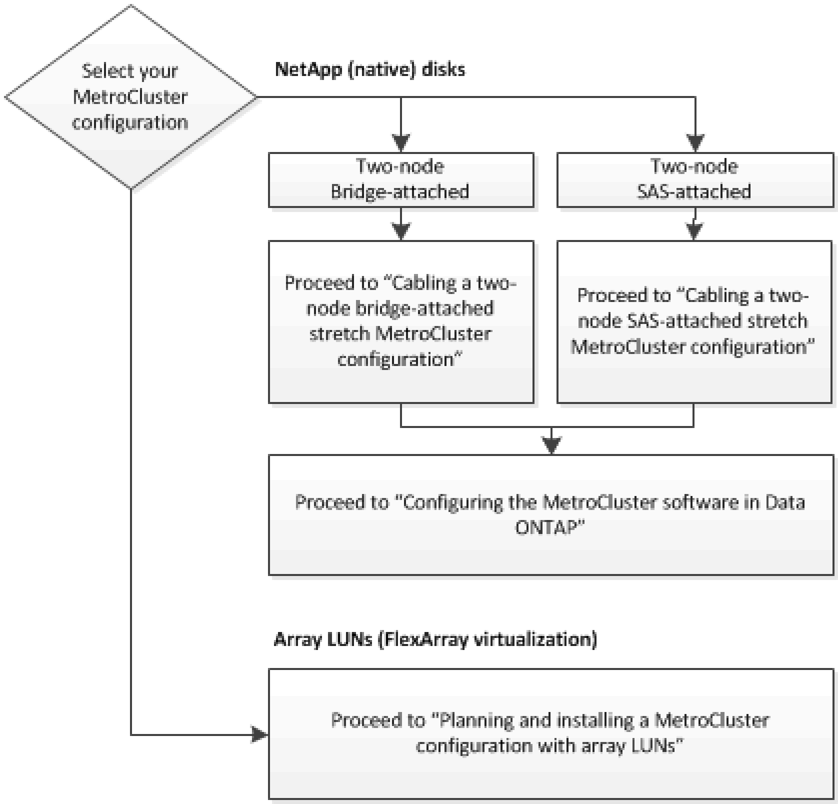
If you are using a firewall at a MetroCluster site, you must ensure access for required ports.

The following table shows TCP/UDP port usage in an external firewall positioned between two MetroCluster sites.

Traffic type	Port/services
Cluster peering	11104 / TCP 11105 / TCP
ONTAP System Manager	443 / TCP
MetroCluster IP intercluster LIFs	65200 / TCP 10006 / TCP and UDP
Hardware assist	4444 / TCP

Choosing the correct installation procedure for your configuration

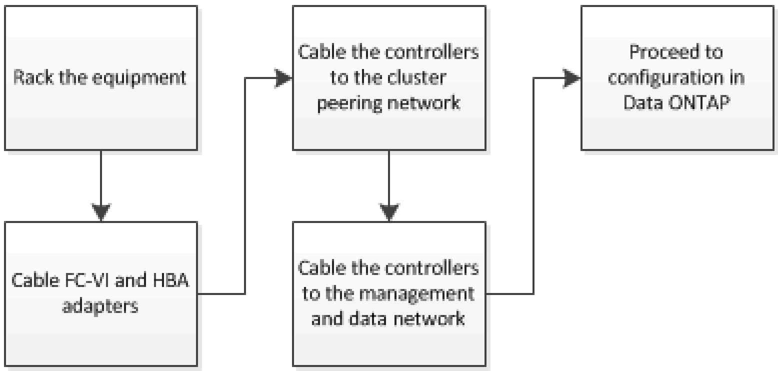
You must choose the correct installation procedure based on whether you are using FlexArray LUNs and how the storage controllers connect to storage shelves.



For this installation type…	Use these procedures…
Two-node stretch configuration with FC-to SAS bridges	1. Cabling a two-node bridge-attached stretch MetroCluster configuration 2. Configuring the MetroCluster software in ONTAP
Two-node stretch configuration with direct-attached SAS cabling	1. Cabling a two-node SAS-attached stretch MetroCluster configuration 2. Configuring the MetroCluster software in ONTAP
Installation with array LUNs	Connections in a stretch MetroCluster configurations with array LUNs

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.



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.

    > 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. 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 components 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
- Site B: controller_B_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

Mixing IOM12 and IOM 6 modules in a stack

Your version of ONTAP must support shelf mixing. Refer to the Interoperability Matrix Tool (IMT) to see if your version of ONTAP supports shelf mixing. NetApp Interoperability

For further details on shelf mixing, see: Hot-adding shelves with IOM12 modules to a stack of shelves with IOM6 modules

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

The storage controllers must be cabled to the storage media 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:

- Prior to installation you must have familiarized yourself with the considerations and best practices for installing and cabling disk shelves for your disk shelf model.
- All MictoCluster components must be supported.

  NetApp Interoperability Matrix Tool

  In the IMT, you can use the Storage Solution field to select your MetroCluster solution. 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.

Racking the hardware components

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

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. Using standard shop practices for working with electrical equipment make sure you are properly grounded.
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.

   > Shelf IDs must be unique for each SAS disk shelf within each MetroCluster DR group (including both sites). When manually setting shelf IDs, you must power-cycle the disk shelf.

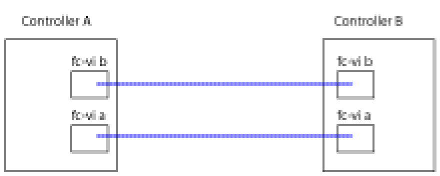
Cabling the controllers to each other and the storage shelves

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.

This task must be performed at both MetroCluster sites.

Steps

1. Cable the FC-VI ports.

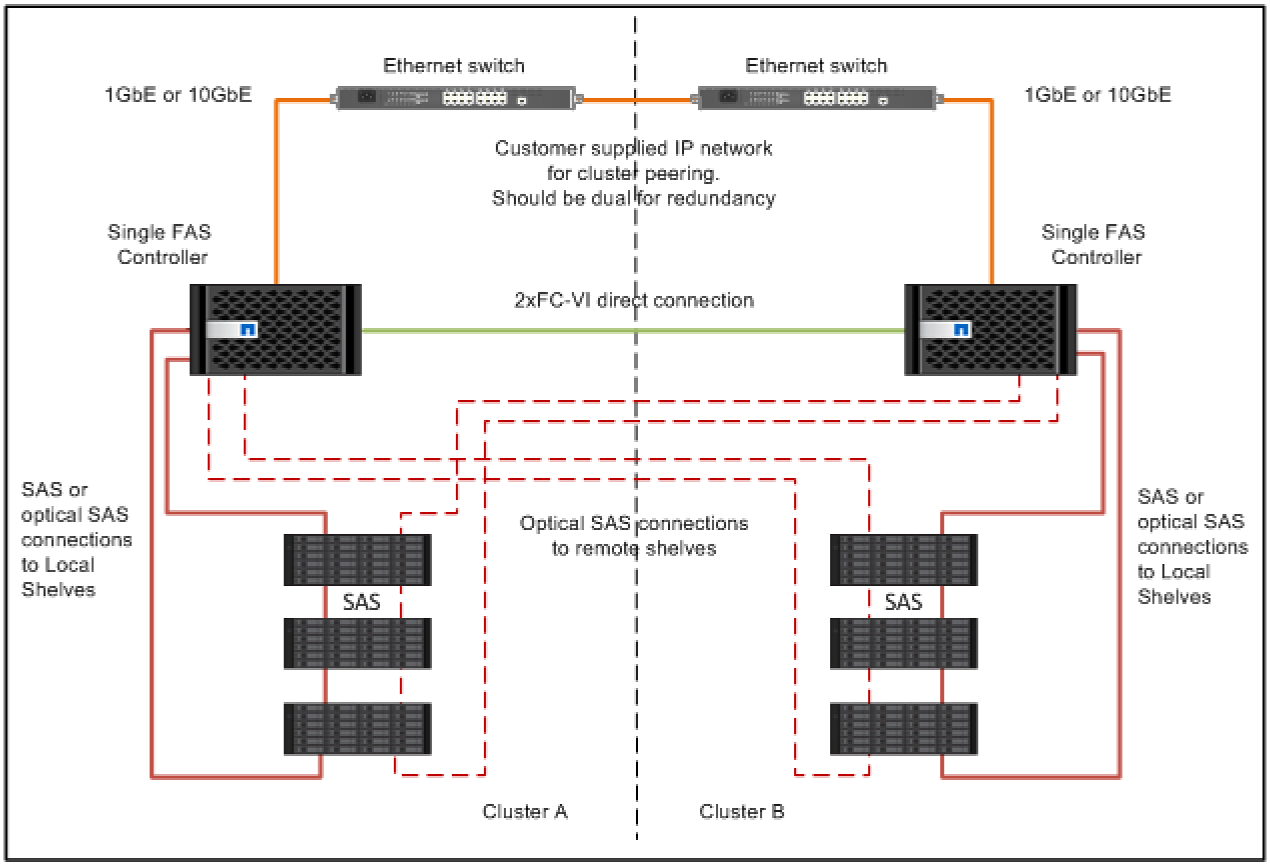


   The above illustration is a typical representative cable connection. The specific FC-VI ports will vary by controller module.

   - FAS8200 and AFF A300 controller modules can be ordered with one of two options for FC-VI connectivity:
     - Onboard ports 0e and 0f are configured in FC-VI mode.
     - Ports 1a and 1b on an FC-VI card go in slot 1.
   - AFF A700 and FAS9000 storage systems controller modules use four FC-VI ports each.
   - AFF A400 and FAS8300 storage system controller modules use FC-VI ports 2a and 2b.

2. Cable the SAS ports.

   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 their partner site.

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.

Steps

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 a 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.

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. In addition you can connect controller to new dedicated network switches such as NetApp CN1601 cluster management switches.

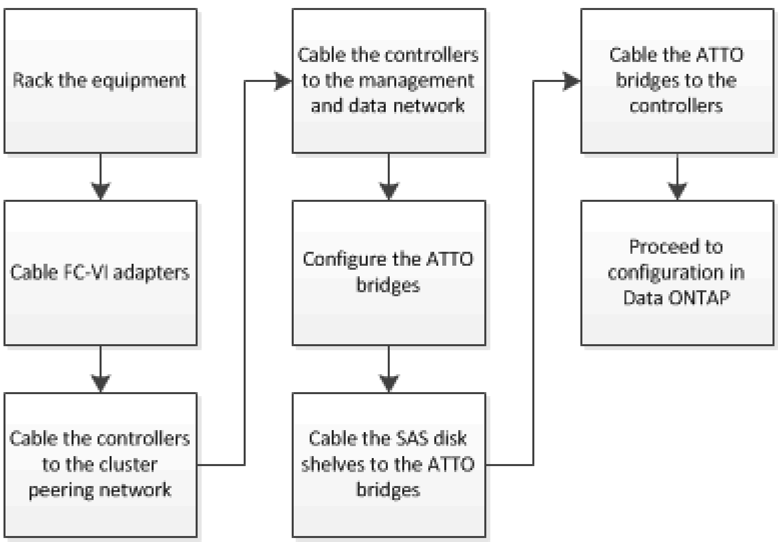
Steps

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.



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.

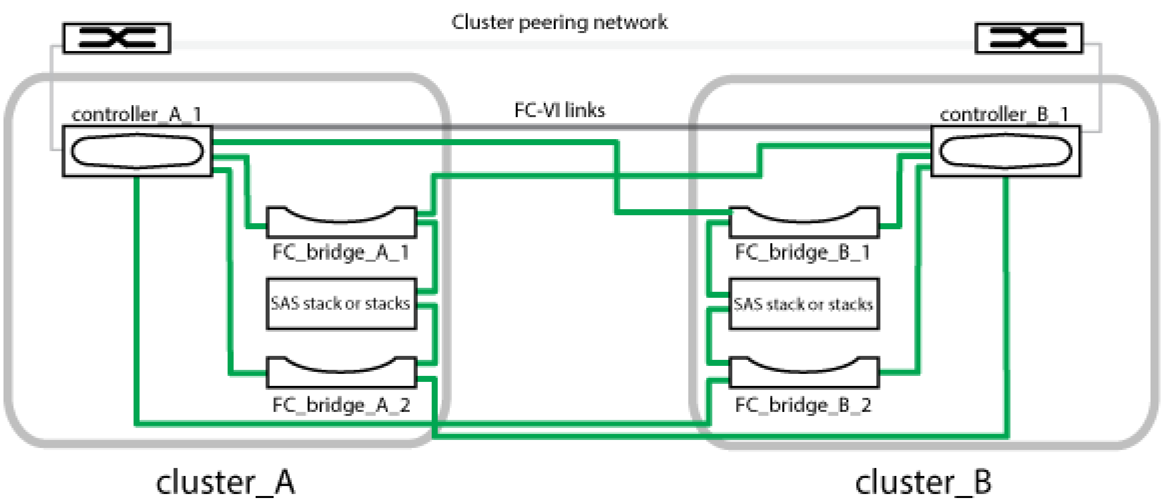
- FC-to-SAS bridges

  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.

  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 6500N bridges are not supported in configurations running ONTAP 9.8 and later.

- 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:
  * bridge_B_1_*port-number*
  * bridge_B_2_*port-number*

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

Mixing IOM12 and IOM 6 modules in a stack

Your version of ONTAP must support shelf mixing. Refer to the Interoperability Matrix Tool (IMT) to see if your version of ONTAP supports shelf mixing. NetApp Interoperability

For further details on shelf mixing, see: Hot-adding shelves with IOM12 modules to a stack of shelves with IOM6 modules

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*.

Site A	Your value
Bridge_A_1a IP address	
Bridge_A_1a Username	
Bridge_A_1a Password	

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*.

Site A	Your value
Bridge_A_1b IP address	
Bridge_A_1b Username	
Bridge_A_1b Password	

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	Your value
Bridge_B_1a IP address	
Bridge_B_1a Username	
Bridge_B_1a Password	

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*.

Site B	Your value
Bridge_B_1b IP address	
Bridge_B_1b Username	
Bridge_B_1b Password	

Installing and cabling MetroCluster components

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

Racking the hardware components

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

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, 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.
   - You must power-cycle each disk shelf.
   - Shelf IDs must be unique for each SAS disk shelf within each MetroCluster DR group (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.

For maximum resiliency, bridges that are attached to the same stack of disk shelves must be connected to different power sources.

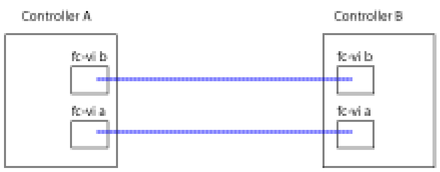
The bridge Ready LED might take up to 30 seconds to illuminate, indicating that the bridge has completed its power-on self test sequence.

Cabling the controllers to each other

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

Steps

1. Cable the FC-VI ports.

   The above illustration is a typical representation of the required cabling. 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 their partner site.

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.

Steps

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 a 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.

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. In addition you can connect controller to new dedicated network switches such as NetApp CN1601 cluster management switches.

Steps

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

   AFF and FAS Documentation Center

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.

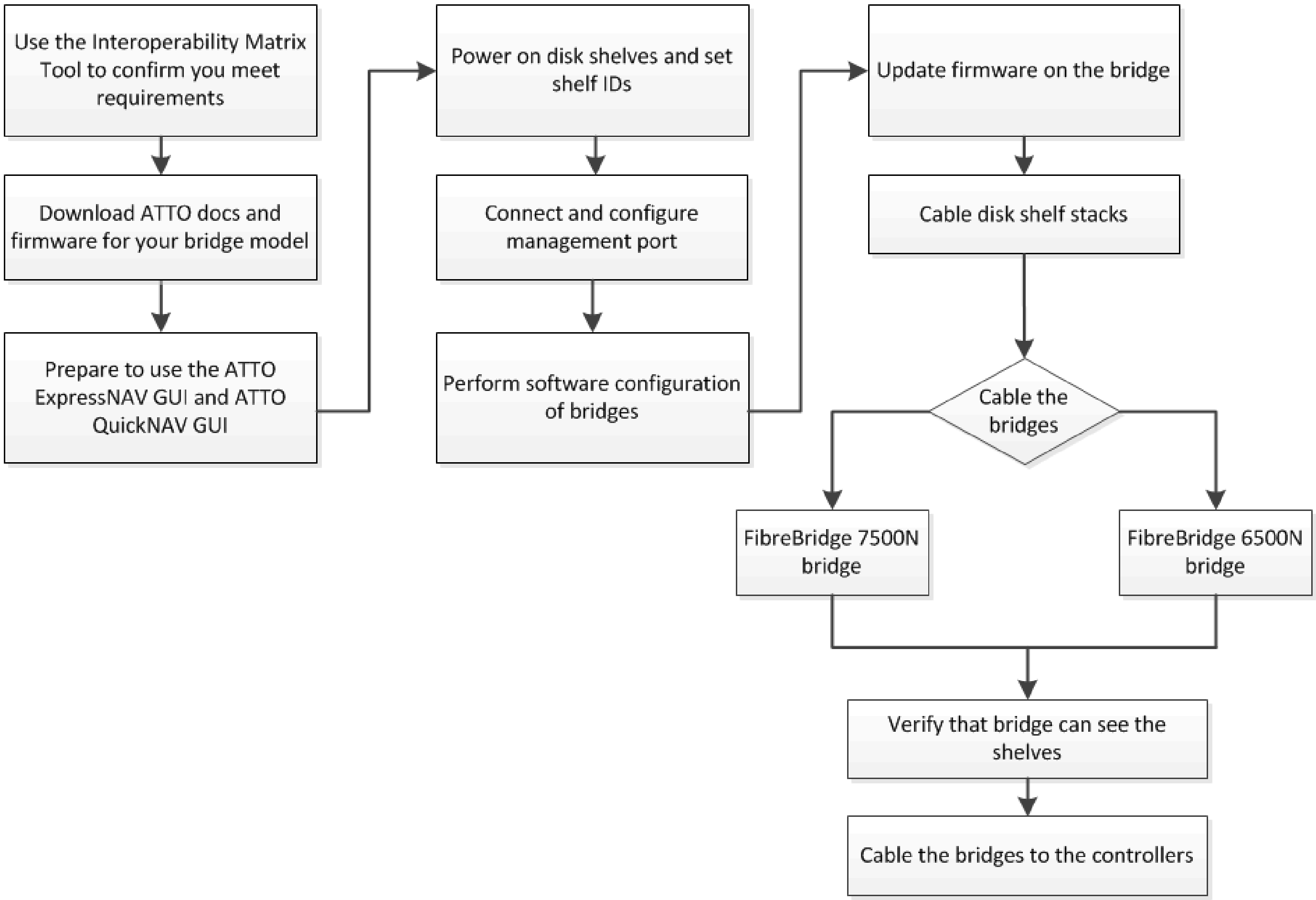
For systems received from the factory, the FC-to-SAS bridges are preconfigured and do not require additional configuration.

This procedure assumes that you are using the recommended bridge management interfaces: the ATTO ExpressNAV GUI and ATTO QuickNAV utility.

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.

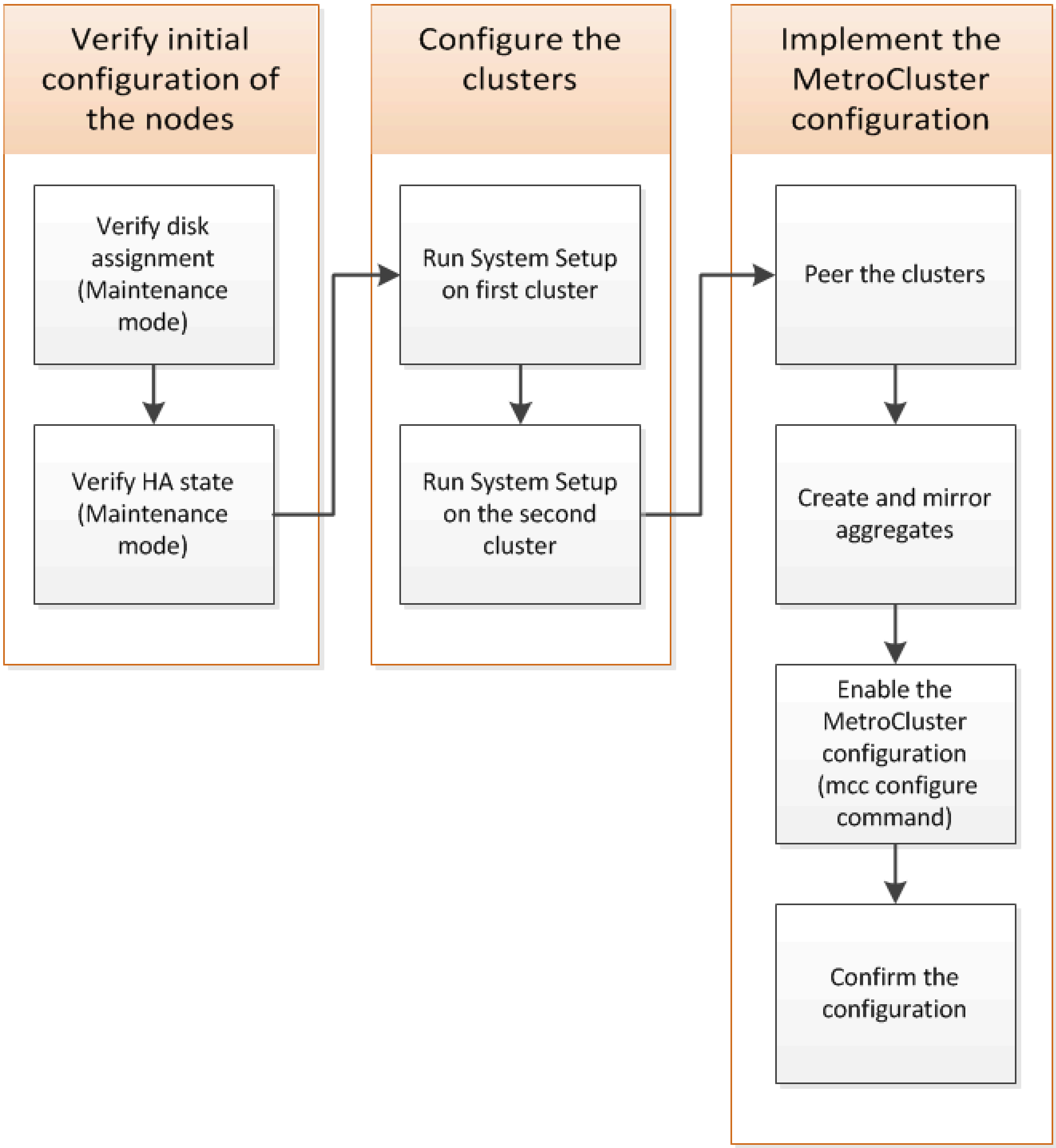
You can use other management interfaces instead, if needed, such as a serial port or Telnet to configure and manage a bridge and to configure the Ethernet management 1 port, and FTP to update the bridge firmware.

This procedure uses the following workflow:



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 You need to gather the required IP addresses for the controller modules before you begin the configuration process.
2. IP network information worksheet for site A

IP network informatin 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:

Type of information	Your values
Cluster nameExample used in this guide: site_A	
DNS domain	
DNS name servers	
Location	
Administrator password	

Site A node information

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

Node	Port	IP address	Network mask	Default gateway
Node 1 Example used in this guide: controller_A_1				
Node 2Not required if using two-node MetroCluster configuration (one node at each site). Example used in this guide: controller_A_2				

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.

Node	Port	IP address of intercluster LIF	Network mask	Default gateway
Node 1 IC LIF 1				
Node 1 IC LIF 2				

Site A time server information

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

Node	Host name	IP address	Network mask	Default gateway
NTP server 1				
NTP server 2				

Site A AutoSupport information

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

Type of information		Your values
From email address		
Mail hosts	IP addresses or names	
Transport protocol	HTTP, HTTPS, or SMTP	
	Proxy server	
Recipient email addresses or distribution lists	Full-length messages	
	Concise messages	
	Partners	

Site A SP information

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

Node	IP address	Network mask	Default gateway
Node 1			

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:

Type of information	Your values
Cluster nameExample used in this guide: site_B	
DNS domain	
DNS name servers	
Location	
Administrator password	

Site B node information

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

Node	Port	IP address	Network mask	Default gateway
Node 1 Example used in this guide: controller_B_1				
Node 2Not required for two-node MetroCluster configurations (one node at each site). Example used in this guide: controller_B_2				

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.

Node	Port	IP address of intercluster LIF	Network mask	Default gateway
Node 1 IC LIF 1				
Node 1 IC LIF 2				

Site B time server information

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

Node	Host name	IP address	Network mask	Default gateway
NTP server 1				
NTP server 2				

Site B AutoSupport information

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

Type of information		Your values
From email address		
Mail hosts	IP addresses or names	
Transport protocol	HTTP, HTTPS, or SMTP	
	Proxy server	
Recipient email addresses or distribution lists	Full-length messages	
	Concise messages	
	Partners	

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:

Node	IP address	Network mask	Default gateway
Node 1 (controller_B_1)			

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.

Configuration step	Standard cluster configuration	MetroCluster configuration
Configure management, cluster, and data LIFs on each node.	Same in both types of clusters	
Configure the root aggregate.	Same in both types of clusters	
Set up the cluster on one node in the cluster.	Same in both types of clusters	
Join the other node to the cluster.	Same in both types of clusters	
Create a mirrored root aggregate.	Optional	Required
Peer the clusters.	Optional	Required
Enable the MetroCluster configuration.	Does not apply	Required

Restoring system defaults and configuring the HBA type on a controller module

To ensure a successful MetroCluster installation, reset and restore defaults on the controller modules.

Important

This task is only required for stretch configurations using FC-to-SAS bridges.

Steps

1. At the LOADER prompt, return the environmental variables to their default setting:

   `set-defaults`

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

   a. Boot into Maintenance mode:

      `boot_ontap maint`

   b. Check the current settings of the ports:

      `ucadmin show`

   c. Update the port settings as needed.

If you have this type of HBA and desired mode…	Use this command…
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter_name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter_name`*

FC target	`fcadmin config -t target` *`adapter_name`*
FC initiator	`fcadmin config -t initiator` *`adapter_name`*

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:

   `boot_ontap maint`

5. Verify the changes you made:

If you have this type of HBA…	Use this command…
CNA	`ucadmin show`
FC	`fcadmin show`

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.

> ⓘ Converting an FC port to an FC-VI port with the ucadmin command is only supported on the FAS8020 and AFF 8020 systems. Converting FC ports to FCVI ports is not supported on any other platform.

Steps

1. Disable the ports:

   `storage disable adapter 1a`

   `storage disable adapter 1b`

```
*> 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`

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        -          offline
  1b     fc       initiator  -        -          offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

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).

```
*> 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

```
*> ucadmin show
         Current  Current    Pending  Pending    Admin
Adapter  Mode     Type       Mode     Type       Status
-------  -------  ---------  -------  ---------  -------
  ...
  1a     fc       initiator  -        fcvi       offline
  1b     fc       initiator  -        fcvi       offline
  1c     fc       initiator  -        -          online
  1d     fc       initiator  -        -          online
```

5. Shut down the controller, and then reboot into Maintenance mode.
6. Confirm the configuration change:

ucadmin show local

```
Node            Adapter  Mode     Type       Mode     Type       Status
------------    -------  -------  ---------  -------  ---------
-----------
...
controller_B_1
                1a       fc       fcvi       -        -          online
controller_B_1
                1b       fc       fcvi       -        -          online
controller_B_1
                1c       fc       initiator  -        -          online
controller_B_1
                1d       fc       initiator  -        -          online
6 entries were displayed.
```

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.

Disk shelf (`example name`)…	**At site…**	**Belongs to…**	**And is assigned to that node's…**
Disk shelf 1 (shelf_A_1_1)	Site A	Node A 1	Pool 0
Disk shelf 2 (shelf_A_1_3)			
Disk shelf 3 (shelf_B_1_1)		Node B 1	Pool 1
Disk shelf 4 (shelf_B_1_3)			
Disk shelf 9 (shelf_B_1_2)	Site B	Node B 1	Pool 0
Disk shelf 10 (shelf_B_1_4)			
Disk shelf 11 (shelf_A_1_2)		Node A 1	Pool 1
Disk shelf 12 (shelf_A_1_4)			

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

Assign these disks in the drawer…	**To this node and pool…**
1 - 6	Local node's pool 0
7 - 12	DR partner's pool 1

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:

   `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:
disk assign -shelf *disk_shelf_name* -p *pool*

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

```
*> 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:
disk assign -shelf *disk_shelf_name* -p *pool*

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

```
*> 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:
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

   Halt the node.

   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 Cluster Setup wizard, and use the `cluster setup` command 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.

   > You must repeat this step on the node at the disaster recovery (DR) site.

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

```
::> 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.

This system will send event messages and periodic 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}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address [10.101.01.01]:

Enter the node management interface netmask [101.010.101.0]:
Enter the node management interface default gateway [10.101.01.0]:



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

2. Create a new cluster: **`create`**
3. Choose whether the node is to be used as a single node cluster.

```
Do you intend for this node to be used as a single node cluster? {yes,
no} [yes]:
```

4. Accept the system default **`yes`** by pressing Enter, or enter your own values by typing **`no`**, and then pressing Enter.
5. 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.

6. After you complete the **Cluster Setup** wizard and it exits, verify that the cluster is active and the first node is healthy:

   `cluster show`

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

```
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.

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.

Related information

Cluster and SVM peering express configuration

Considerations when using dedicated ports

Considerations when sharing data ports

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.

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.

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

```
cluster01::> network port show
                                                             Speed
(Mbps)
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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

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.

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

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port

Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

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*

   The following example assigns ports e0e and e0f to the failover group intercluster01 on the system SVMcluster01:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verify that the failover group was created:

   network interface failover-groups show

   For complete command syntax, see the man page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

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

ONTAP version	Command
9.6 and later	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home-port port -address port_IP -netmask netmask -failover-group failover_group`
9.5 and earlier	`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.

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

+

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-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 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

1. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

2. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster -failover`

In ONTAP 9.6 and later:
In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

The following example shows that the intercluster LIFs `cluster01_icl01` and `cluster01_icl02` on the SVMe0e port will fail over to the `e0f` port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Related information

Considerations when using dedicated ports

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.

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

```
cluster01::> network port show
                                                                    Speed
(Mbps)
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:

In ONTAP 9.6 and later:
network interface create -vserver *system_SVM* -lif *LIF_name* -service-policy default-intercluster -home-node node -home-port *port* -address *port_IP* -netmask *netmask*
In ONTAP 9.5 and earlier:
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.

The following example creates intercluster LIFs cluster01_icl01 and cluster01_icl02:

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

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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:

In ONTAP 9.6 and later:

`network interface show -service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

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

```
cluster01::> network interface show -service-policy default-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 information

[Considerations when sharing data ports]

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.

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.

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

```
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.

   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:

```
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

```
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

```
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
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             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.

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.

   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:

   ```
   cluster02::> cluster peer create -peer-addrs
   192.168.2.201,192.168.2.202
   Enter the passphrase:
   Please enter the passphrase again:
   ```

   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.

   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
   Please confirm the passphrase:
   Please confirm the passphrase again:
   ```

   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.

```
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.

```
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
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             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`

> 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`

   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

     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.

     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

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.

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:

   `storage disk show -spare -owner` ***`node_name`***

2. Create the aggregate:

   `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.

  The following command creates a unmirrored aggregate with 10 disks:

  ```
  controller_A_1::> storage aggregate create aggr1_controller_A_1
  -diskcount 10 -node controller_A_1
  [Job 15] Job is queued: Create aggr1_controller_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`***

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.

  > If you want to use a single mirrored data aggregate, then see step 1 for instructions.

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

About this task

You can 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:

If your MetroCluster configuration has…	Then do this…
Multiple data aggregates	From any node's prompt, configure MetroCluster: **`metrocluster configure`** ***`node-name`***

If your MetroCluster configuration has…	Then do this…
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`**

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:

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

[Job 121] Job succeeded: Configure is successful.
```

2. Verify the networking status on site A:

`network port show`

The following example shows the network port usage:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000

7 entries were displayed.
```

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

   a. Verify the configuration from site A:
   `metrocluster show`

```
cluster_A::> metrocluster show

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Verify the configuration from site B:
   `metrocluster show`

```
cluster_B::> metrocluster show
Cluster                    Entry Name          State
-------------------------- ------------------- -----------
 Local: cluster_B          Configuration state configured
                           Mode                normal
                           AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A          Configuration state configured
                           Mode                normal
                           AUSO Failure Domain auso-on-cluster-
disaster
```

Configuring SNMPv3 in a MetroCluster configuration

The authentication and privacy protocols on the switches and on the ONTAP system must be the same.

ONTAP currently supports AES-128 and AES-256 encryption.

Steps

1. Create an SNMP user for each switch from the controller prompt:

   `security login create`

   ```
   Controller_A_1::> security login create -user-or-group-name snmpv3user
   -application snmp -authentication-method usm -role none -remote-switch
   -ipaddress 10.10.10.10
   ```

2. Respond to the following prompts as required at your site:

```
Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256) [none]: sha

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128) [none]:
aes128

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:
```

> The same username can be added to different switches with different IP addresses.

3. Create an SNMP user for the rest of the switches.

   The following example shows how to create a username for a switch with the IP address 10.10.10.11.

```
Controller_A_1::> security login create -user-or-group-name snmpv3user
-application snmp -authentication-method usm -role none -remote-switch
-ipaddress 10.
10.10.11
```

4. Check that there is one login entry for each switch:

   `security login show`

```
Controller_A_1::> security login show -user-or-group-name snmpv3user
-fields remote-switch-ipaddress

vserver      user-or-group-name application authentication-method
remote-switch-ipaddress

------------ ------------------ ----------- ---------------------
-----------------------

node_A_1 SVM 1 snmpv3user     snmp        usm
10.10.10.10

node_A_1 SVM 2 snmpv3user     snmp        usm
10.10.10.11

node_A_1 SVM 3 snmpv3user    snmp        usm
10.10.10.12

node_A_1 SVM 4 snmpv3user     snmp        usm
10.10.10.13

4 entries were displayed.
```

5. Configure SNMPv3 on the switches from the switch prompt:

   `snmpconfig --set snmpv3`

   If you require RO access, after 'User (ro):' specify the 'snmpv3user' as shown in the example:

```
Switch-A1:admin> snmpconfig --set snmpv3
SNMP Informs Enabled (true, t, false, f): [false] true
SNMPv3 user configuration(snmp user not configured in FOS user database
will have physical AD and admin role as the default):
User (rw): [snmpadmin1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [2]
Engine ID: [00:00:00:00:00:00:00:00:00]
User (ro): [snmpuser2] snmpv3user
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [2]
Priv Protocol [DES(1)/noPriv(2)/AES128(3)/AES256(4)]): (2..2) [3]
```

   The example shows how to configure a read-only user. You can adjust the RW users if needed. You should also set passwords on unused accounts to secure them and use the best encryption available in your ONTAP release.

6. Configure encryption and passwords on the remaining switch users as required on your site.

Configuring FC-to-SAS bridges for health monitoring

In systems running ONTAP versions prior to 9.8, 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.

- Third-party SNMP monitoring tools are not supported for FibreBridge bridges.
- Starting with ONTAP 9.8, FC-to-SAS bridges are monitored via in-band connections by default, and additional configuration is not required.

> Starting with ONTAP 9.8, the **`storage bridge`** command is replaced with **`system bridge`**. The following steps show the **`storage bridge`** command, but if you are running ONTAP 9.8 or later, the **`system bridge`** command is preferred.

Steps

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

ONTAP version	Command
9.5 and later	**`storage bridge add -address 0.0.0.0 -managed-by in-band -name`** ***`bridge-name`***
9.4 and earlier	**`storage bridge add -address`** ***`bridge-ip-address`*** **`-name`** ***`bridge-name`***

   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.

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

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status
Vendor Model                Bridge WWN
------------------  ------------- ------------  --------------
------ -----------------    ----------
ATTO_10.10.20.10  atto01        true          ok             Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok             Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok             Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok             Atto
FibreBridge 7500N      2000001086703b80

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.

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.

1. Check the configuration:

   `metrocluster check run`

   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.

   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

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr1
```

```
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                       controller_A_1_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok


controller_A_2         controller_A_2_aggr0
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                       controller_A_2_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                       controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

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

Cluster               Check                            Result
--------------------- ------------------------------- ---------
mccint-fas9000-0102
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
mccint-fas9000-0304
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
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.

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.

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

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.

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

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.

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

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

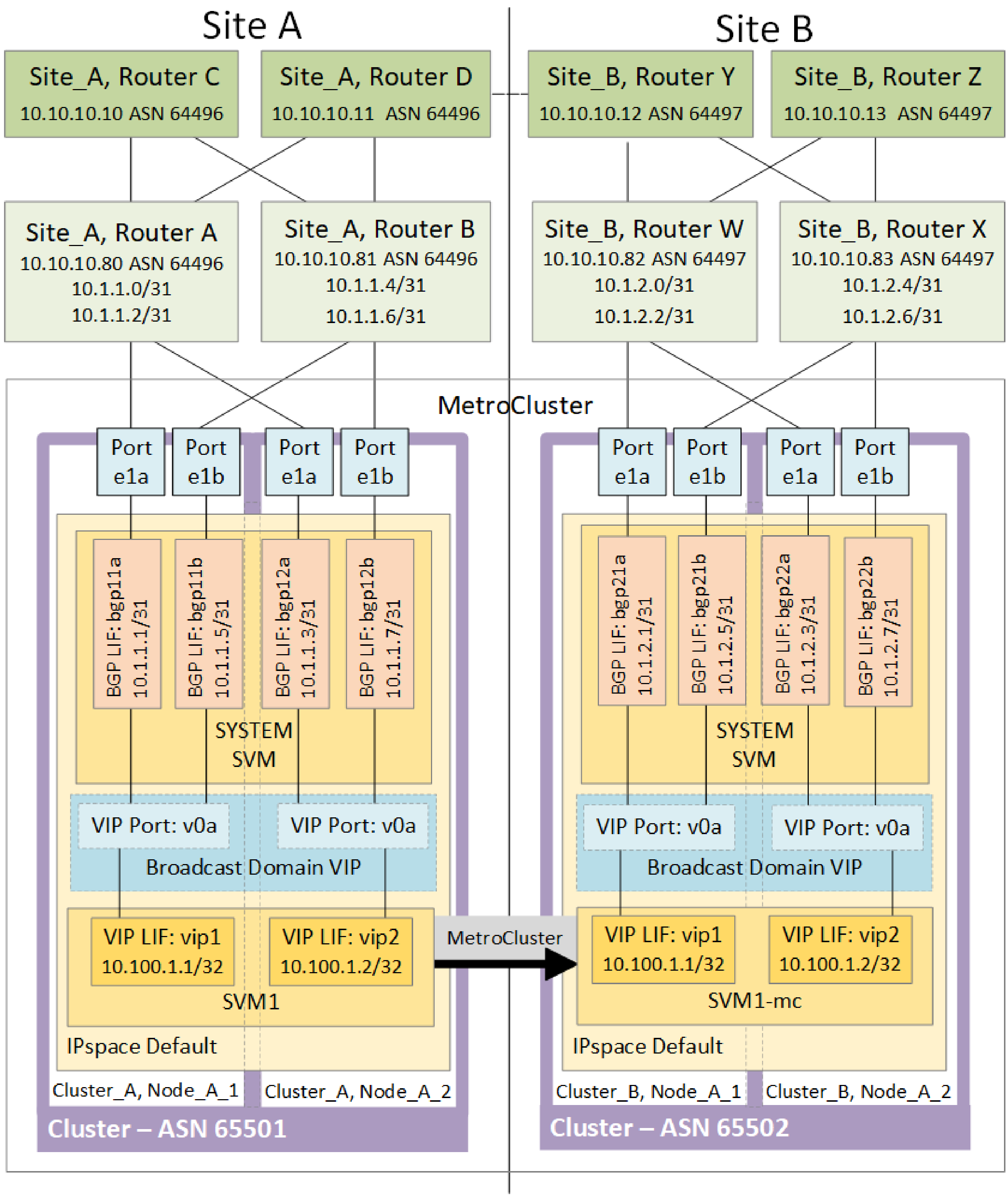
   The System Administration Guide contains additional information under the section *Managing configuration backups*.

Considerations for using virtual IP and Border Gateway Protocol with a MetroCluster configuration

Starting with ONTAP 9.5, ONTAP supports layer 3 connectivity using virtual IP (VIP) and Border Gateway Protocol (BGP). The combination VIP and BGP for redundancy in the front-end networking with the back-end MetroCluster redundancy provides a layer 3 disaster recovery solution.

Review the following guidelines and illustration when planning your layer 3 solution. For details on implementing VIP and BGP in ONTAP, refer to the following section:

Configuring virtual IP (VIP) LIFs



ONTAP limitations

ONTAP does not automatically verify that all nodes on both sites of the MetroCluster configuration are configured with BGP peering.

ONTAP does not perform route aggregation but announces all individual virtual LIF IPs as unique host routes at all times.

ONTAP does not support true AnyCast — only a single node in the cluster presents a specific virtual LIF IP (but is accepted by all physical interfaces, regardless of whether they are BGP LIFs, provided the physical port is part of the correct IPspace). Different LIFs can migrate independently of each other to different hosting nodes.

Guidelines for using this Layer 3 solution with a MetroCluster configuration

You must configure your BGP and VIP correctly to provide the required redundancy.

Simpler deployment scenarios are preferred over more complex architectures (for example, a BGP peering router is reachable across an intermediate, non-BGP router). However, ONTAP does not enforce network design or topology restrictions.

VIP LIFs only cover the frontend/data network.

Depending on your version of ONTAP, you must configure BGP peering LIFs in the node SVM, not the system or data SVM. In ONTAP 9.8, the BGP LIFs are visible in the cluster (system) SVM and the node SVMs are no longer present.

Each data SVM requires the configuration of all potential first hop gateway addresses (typically, the BGP router peering IP address), so that the return data path is available if a LIF migration or MetroCluster failover occurs.

BGP LIFs are node specific, similar to intercluster LIFs — each node has a unique configuration, which does not need to be replicated to DR site nodes.

The existence of the v0a (v0b and so on.) continuously validates the connectivity, guaranteeing that a LIF migrate or failover succeeds (unlike L2, where a broken configuration is only visible after the outage).

A major architectural difference is that clients should no longer share the same IP subnet as the VIP of data SVMs. An L3 router with appropriate enterprise grade resiliency and redundancy features enabled (for example, VRRP/HSRP) should be on the path between storage and clients for the VIP to operate correctly.

The reliable update process of BGP allows for smoother LIF migrations because they are marginally faster and have a lower chance of interruption to some clients.

You can configure BGP to detect some classes of network or switch misbehaviors faster than LACP, if configured accordingly.

External BGP (EBGP) uses different AS numbers between ONTAP node(s) and peering routers and is the preferred deployment to ease route aggregation and redistribution on the routers. Internal BGP (IBGP) and the use of route reflectors is not impossible but outside the scope of a straightforward VIP setup.

After deployment, you must check that the data SVM is accessible when the associated virtual LIF is migrated between all nodes on each site (including MetroCluster switchover) to verify the correct configuration of the static routes to the same data SVM.

VIP works for most IP-based protocols (NFS, SMB, iSCSI).

Testing the MetroCluster configuration

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

Verifying negotiated switchover

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

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 the command is issued from will switch over the partner site.

For MetroCluster IP configurations:

- For ONTAP 9.4 and earlier:
  - Mirrored aggregates will become degraded after the negotiated switchover.
- For ONTAP 9.5 and later:
  - Mirrored aggregates will remain in normal state if the remote storage is accessible.
  - Mirrored aggregates will become degraded after the negotiated switchover if access to the remote storage is lost.
- For ONTAP 9.8 and later:
  - Unmirrored aggregates that are located at the disaster site will become unavailable if access to the remote storage is lost. This might lead to a controller outage.

Steps

1. Confirm that all nodes are in the configured state and normal mode:

   `metrocluster node show`

   ```
   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`

```
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`

```
cluster_A::>  metrocluster node show

Cluster                        Configuration State    Mode
------------------------------ ----------------------
------------------------
Local: cluster_A                configured             switchover
Remote: cluster_B               not-reachable          -
              configured             normal
```

4. Confirm that the switchover operation was successful:

   `metrocluster operation show`

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

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.

This test should take about 30 minutes.

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

Steps

1. Verify that healing is completed:

   `metrocluster node show`

   The following example shows the successful completion of the command:

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1          configured     enabled   heal roots
completed
      cluster_B
              node_B_2          unreachable    -         switched over
42 entries were displayed.metrocluster operation show
```

2. Verify that all aggregates are `mirrored`:

   `storage aggregate show`

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

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                              mirrored,
                                                              normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                              mirrored,
                                                              normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                              mirrored,
                                                              normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

3. Boot nodes from the disaster site.
4. Check the status of switchback recovery:

`metrocluster node show`

```
cluster_A::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
             node_A_1            configured     enabled   heal roots
completed
      cluster_B
             node_B_2            configured     enabled   waiting for
switchback
                                                          recovery
2 entries were displayed.
```

5. Perform the switchback:

   metrocluster switchback

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

6. Confirm status of the nodes:

   metrocluster node show

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

2 entries were displayed.
```

7. Confirm status of the metrocluster operation:

   metrocluster operation show

   The output should show a successful state.

```
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.

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.

> Starting with ONTAP 9.8, the **`storage bridge`** command is replaced with **`system bridge`**. The following steps show the **`storage bridge`** command, but if you are running ONTAP 9.8 or later, the **`system bridge`** command is preferred.

Steps

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

   `storage bridge show`

   ```
   cluster_A::> storage bridge show

                                                               Is
   Monitor
   Bridge     Symbolic Name Vendor  Model     Bridge WWN       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`

```
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.

The best practice is for each power supply unit (PSU) in a component to be connected to a separate power supply. If both PSUs are connected to the same power distribution unit (PDU) and an electrical disruption occurs, the site could down and 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 PDUs are disconnected.
- No failover or loss of service should occur.

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.

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

Node Sensor              State Value/Units Crit-Low Warn-Low Warn-Hi
Crit-Hi
---- --------------------- ------ ----------- -------- -------- -------
-------
node_A_1
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
node_A_2
        PSU1            fault
                            PSU_OFF
        PSU1 Pwr In OK  fault
                            FAULT
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.

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

```
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

```
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*

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

cluster_A::> vserver show -type data
                               Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

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
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

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.

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

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 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)
                                                              Usable
Physical
     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)
                                                              Usable
Physical
     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)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                              Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                      0   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 *`

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

   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,

mirror

degraded
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,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(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)
                                                              Usable
Physical
     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 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                               Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                         -   -          -  827.7GB
- (failed)
     parity   FAILED                         -   -          -  827.7GB
- (failed)
     data     FAILED                         -   -          -  827.7GB
- (failed)
     data     FAILED                         -   -          -  827.7GB
- (failed)
     data     FAILED                         -   -          -  827.7GB
- (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                               Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                        0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                        0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     data     2.30.21                         0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                         0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                         0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

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*

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

cluster_A::> vserver show -type data
                              Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

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
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Physically power on the shelf.

   Resynchronization starts automatically.

9. Verify that resynchronization has started:

   storage aggregate show

   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

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_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,

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 LUN configurations arrays, 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 HBA port 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:

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.

Direct Attach support for Stretch MetroCluster Configuration with NetApp E-Series array

Except for connecting the FC-VI ports, the rest of this procedure is for setting up a MetroCluster configuration with array LUNs, that are not using E-Series array LUNs. This requires FC switches that are 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

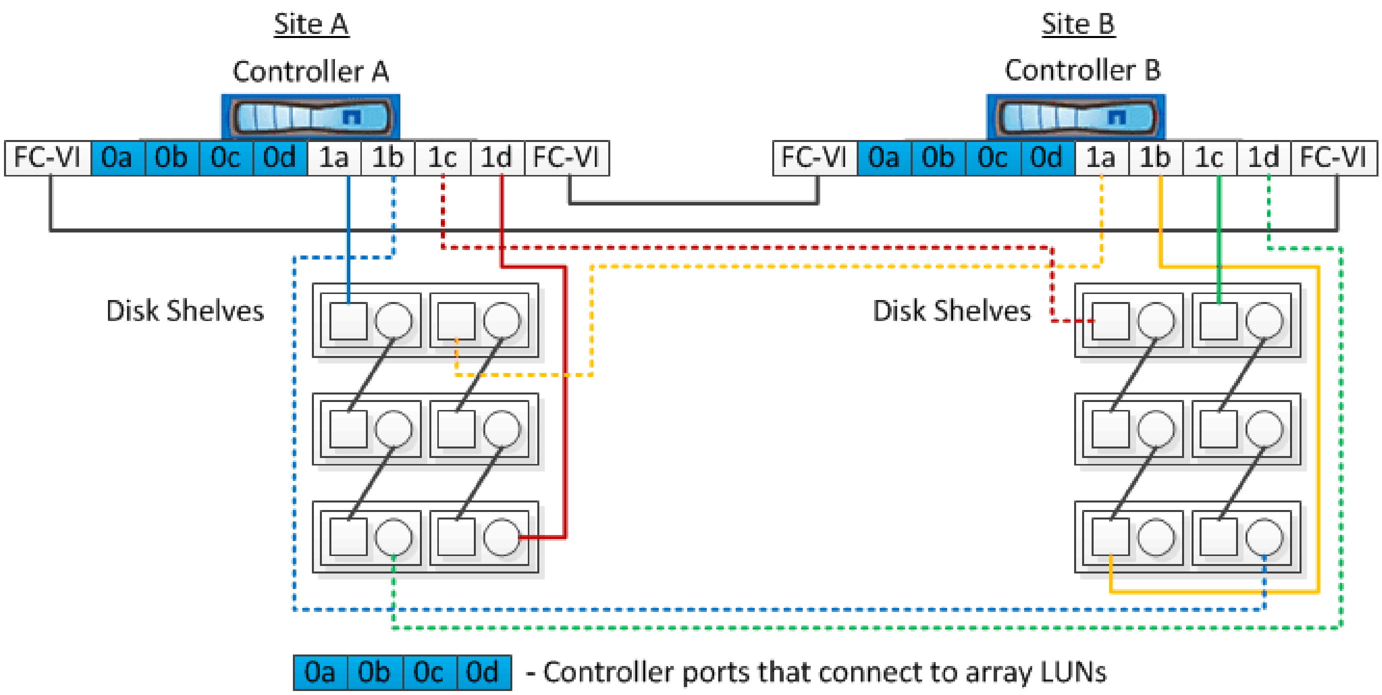
For setting up a stretch MetroCluster configuration with native disks and array LUNs, you must use either FC-to-SAS bridges or SAS optical cables to connect the ONTAP systems to the disk shelves. In addition FC switches must be used for connecting array LUNs to the ONTAP systems.

A minimum of eight HBA ports are required for an ONTAP system to connect to both native disks and array LUNs.

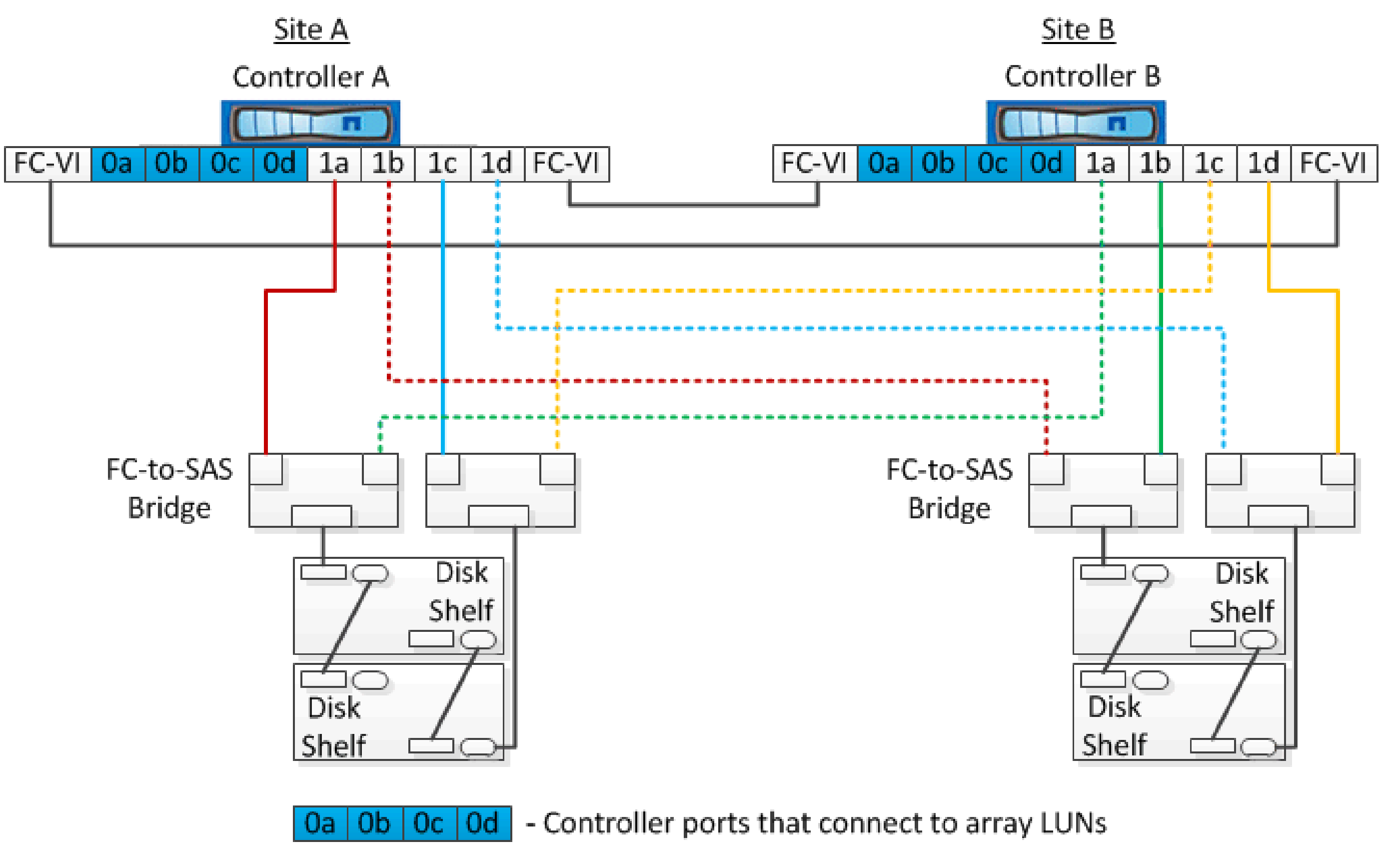
In the following examples representing two-node stretch MetroCluster configurations with disks and array

LUNs, HBA ports 0a through 0d are used for connection with array LUNs. HBA ports 1a through 1d are used for connections with native disks.

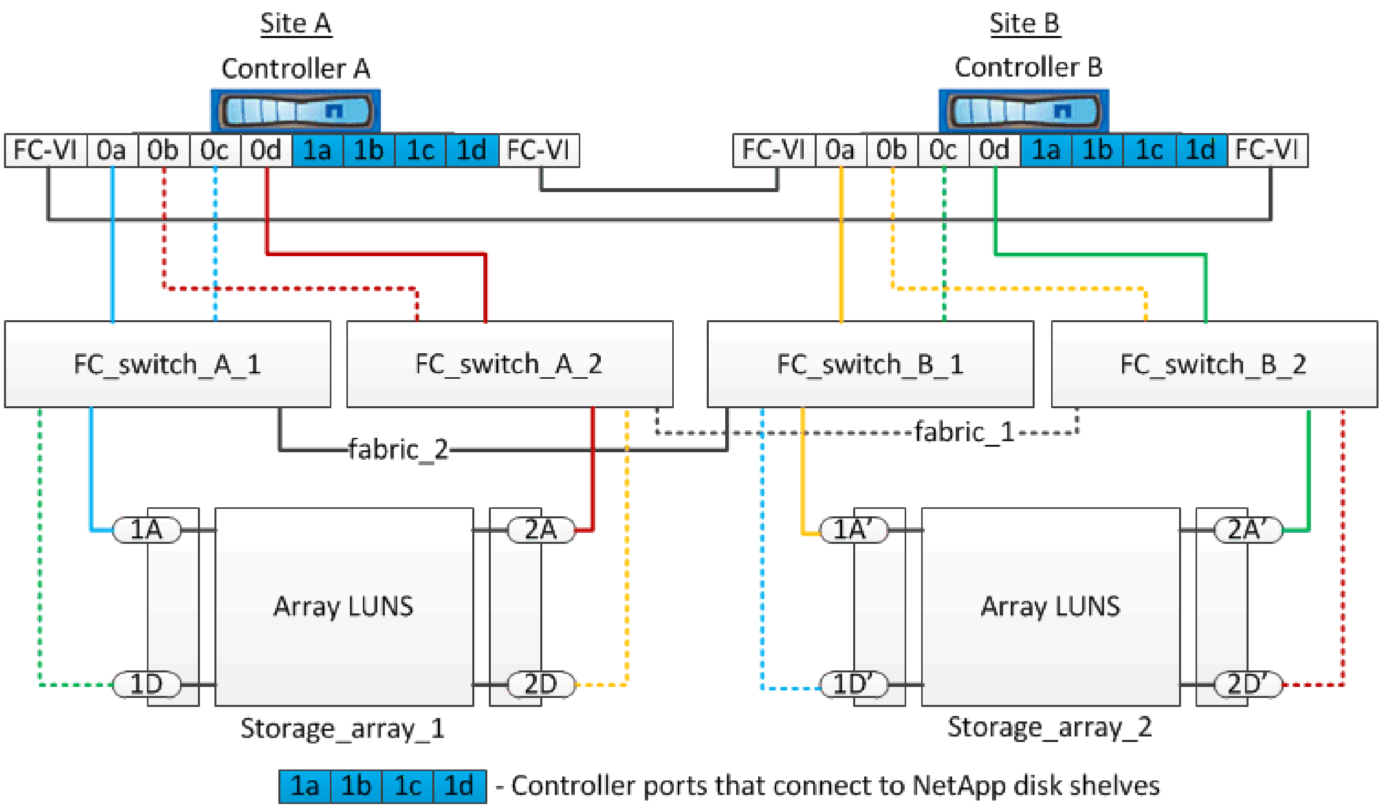
The following illustration shows a two-node stretch MetroCluster configuration in which the native disks are connected to the ONTAP systems using SAS optical cables:



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



The following illustration shows a two-node stretch MetroCluster configuration with the array LUN connections:



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 an 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.

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.

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 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.

Verify that you have downloaded and installed System Manager. System Manager is available from the NetApp Support Site.

- You cannot modify the time zone settings for a failed node or the partner node after 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.

MetroCluster operations in ONTAP System Manager

Depending on your ONTAP version, some MetroCluster specific operations can be performed using ONTAP System Manager.

- Switchover and switchback in MetroCluster IP configurations (starting in ONTAP 9.7).
- Provision and grow of mirrored aggregates in the MetroCluster IP configurations (starting in ONTAP 9.8).

  Unmirrored aggregates are not supported in System Manager.

FlexCache support in a MetroCluster configuration

Starting with ONTAP 9.7, FlexCache volumes are supported on MetroCluster configurations. You should be aware of requirements for manual repeering after switchover or switchback operations.

SVM repeering after switchover when FlexCache origin and cache are within the same MetroCluster site

After a negotiated or unplanned switchover, any SVM FlexCache peering relationship within the cluster must be manually configured.

For example, SVMs vs1 (cache) and vs2 (origin) are on site_A. These SVMs are peered.

After switchover, SVMs vs1-mc and vs2-mc are activated at the partner site (site_B). They must be manually repeered for FlexCache to work using the `vserver peer repeer` command.

SVM repeering after switchover or switchback when a FlexCache destination is on a third cluster and in disconnected mode

For FlexCache relationships to a cluster outside of the MetroCluster configuration, the peering must always be manually reconfigured after a switchover when the clusters involved are in a disconnected mode during switchover.

For example:

- One end of the FlexCache (cache_1 on vs1) resides on MetroCluster site_A has one end of the FlexCache
- The other end of the FlexCache (origin_1 on vs2) resides on site_C (not in the MetroCluster configuration)

When switchover is triggered, and if site_A and site_C are not connected, you must manually repeer the SVMs on site_B (the switchover cluster) and site_C using the `vserver peer repeer` command after the switchover.

When switchback is performed, you must again repeer the SVMs on site_A (the original cluster) and site_C.

FabricPool support in MetroCluster configurations

Starting with ONTAP 9.7, MetroCluster configurations support FabricPool storage tiers.

For general information on using FabricPools, see the Disks and Aggregates Power Guide.

Considerations when using FabricPools

- The clusters must have FabricPool licenses with matching capacity limits.
- The clusters must have IPSpaces with matching names.

  This can be the default IPSpace, or an IP space an administer has created. This IPSpace will be used for FabricPool object store configuration setups.

- For the selected IPSpace, each cluster must have an intercluster LIF defined that can reach the external object store

Configuring an aggregate for use in a mirrored FabricPool

> Before you configure the aggregate you must set up object stores as described in "Setting up object stores for FabricPool in a MetroCluster configuration" in the Disks and Aggregates Power Guide.

To configure an aggregate for use in a FabricPool:

1. Create the aggregate or select an existing aggregate.
2. Mirror the aggregate as a typical mirrored aggregate within the MetroCluster configuration.
3. Create the FabricPool mirror with the aggregate, as described in the Disks and Aggregates Power Guide:
   a. Attach a primary object store.

      This object store is physically closer to the cluster.

   b. Add a mirror object store.

      This object store is physically further away from the cluster than the primary object store.

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).

> 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                     Broadcast                   Avail/
Name      Subnet           Domain    Gateway           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                     Broadcast                   Avail/
Name      Subnet           Domain    Gateway           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

- NFS and SAN configurations: You must use different storage virtual machines (SVMs) for both the unmirrored and mirrored aggregates

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:

Condition	LIF type: FC	LIF type: IP/iSCSI
Node identification	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.	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.
Port identification	ONTAP identifies the connected FC target ports on the DR cluster.	The ports on the DR cluster that are in the same IPspace as the source LIF are selected for a reachability check. If there are no ports in the DR cluster in the same IPspace, the LIF cannot be placed. All of the ports in the DR cluster that are already hosting a LIF in the same IPspace and subnet are automatically marked as reachable; and can be used for placement. These ports are not included in the reachability check.

Condition	LIF type: FC	LIF type: IP/iSCSI
Reachability check	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.	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.
Port selection	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.	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.
LIF placement	From the reachable ports, ONTAP selects the least loaded port for placement.	From the selected ports, ONTAP selects the least loaded port for placement.

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.

> 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.

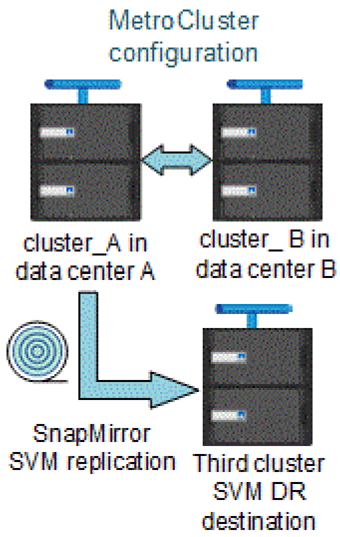
You should be aware of the following requirements and limitations of using SVMs with SnapMirror disaster recovery:

- 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.

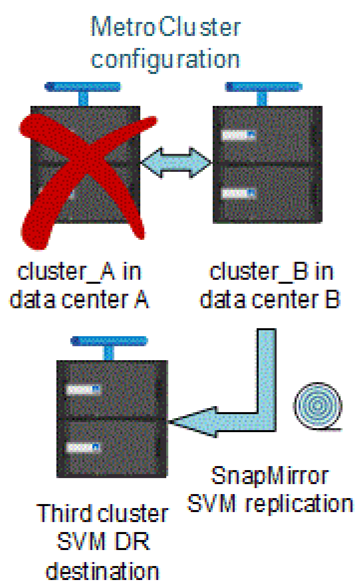
- When a MetroCluster configuration is in a steady state, the MetroCluster sync-destination SVM cannot be the source of an SVM disaster recovery relationship, since the volumes are not online.

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:



- During the switchover and switchback processes, replication to the SVM DR destination might fail.

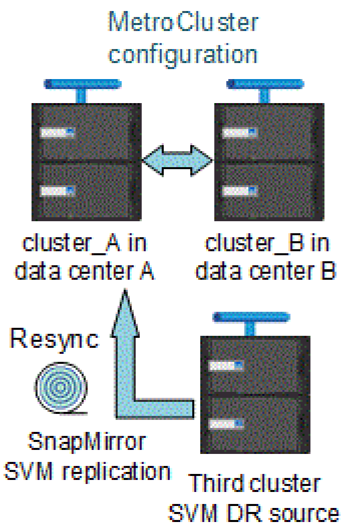
  However, after the switchover or switchback process completes, the next SVM DR scheduled updates will succeed.

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

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.

> 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.

Steps

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`**

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.

- You must disable 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.

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.

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.

   > 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 xref:./install-stretch/ Fabric-attached MetroCluster Installation and Configuration Guide.

   a. Enter advanced privilege mode: + **`set -privilege advanced`**
   b. Refresh the MetroCluster configuration: + **`metrocluster configure -refresh true`**

      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 the MetroCluster configuration and operation from the NetApp documentation library.

MetroCluster and miscellaneous guides

Guide	Content
ONTAP 9 Documentation Center	• All MetroCluster guides
	• A technical overview of the MetroCluster FC configuration and operation. • 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 (DR)
Maintain MetroCluster Components	• Guidelines for maintenance in a MetroCluster FC configuration • Hardware replacement or upgrade. Firmware upgrade procedures for FC-to-SAS bridges and FC switches • Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Replacing hardware at a disaster recovery site in a fabric-attached or stretch MetroCluster FC configuration • Expanding a two-node fabric-attached or stretch MetroCluster FC configuration to a four-node MetroCluster configuration. • Expanding a four-node fabric-attached or stretch MetroCluster FC configuration to an eight-node MetroCluster FC configuration.
MetroCluster Transition Guide MetroCluster Upgrade and Expansion Guide	• Upgrading or refreshing a MetroCluster configuration • Transitioning from a MetroCluster FC configuration to a MetroCluster IP configuration • Expanding a MetroCluster configuration by adding additional nodes
MetroCluster Tiebreaker Software Installation and Configuration Guide	• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software

Active IQ Unified Manager documentation NetApp Documentation: Product Guides and Resources	• Monitoring the MetroCluster configuration and performance
Copy-based transition	• Transitioning data from 7-Mode storage systems to clustered storage systems
ONTAP concepts	• How mirrored aggregates work

MetroCluster Tiebreaker Software Installation and Configuration Guide

This guide describes how to install and configure the MetroCluster Tiebreaker software.

You should use this guide for installing the MetroCluster Tiebreaker software.

Overview of the Tiebreaker software

It is helpful to understand what the NetApp MetroCluster Tiebreaker software is and how it distinguishes between types of failures so that you can monitor your MetroCluster configurations efficiently. You use the Tiebreaker CLI to manage settings and monitor the status and operations of MetroCluster configurations.

Detecting failures with NetApp MetroCluster Tiebreaker software

The Tiebreaker software resides on a Linux host. You need the Tiebreaker software only if you want to monitor 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, from a site failure.

After you install the Tiebreaker software on a Linux host, you can configure the clusters in a MetroCluster configuration to monitor for disaster conditions.

How the Tiebreaker software detects site failures

The NetApp MetroCluster Tiebreaker software checks the reachability of the nodes in a MetroCluster configuration and the cluster to determine whether a site failure has occurred. The Tiebreaker software also triggers an alert under certain conditions.

Components monitored by the Tiebreaker software

The Tiebreaker software monitors each controller in the MetroCluster configuration by establishing redundant connections through multiple paths to a node management LIF and to the cluster management LIF, both hosted on the IP network.

The Tiebreaker software monitors the following components in the MetroCluster configuration:

- Nodes through local node interfaces
- Cluster through the cluster-designated interfaces
- Surviving cluster to evaluate whether it has connectivity to the disaster site (NV interconnect, storage, and intercluster peering)

When there is a loss of connection between the Tiebreaker software and all of the nodes in the cluster and to the cluster itself, the cluster will be declared as “not reachable” by the Tiebreaker software. It takes around three to five seconds to detect a connection failure. If a cluster is unreachable from the Tiebreaker software, the surviving cluster (the cluster that is still reachable) must indicate that all of the links to the partner cluster are severed before the Tiebreaker software triggers an alert.

> All of the links are severed if the surviving cluster can no longer communicate with the cluster at the disaster site through FC (NV interconnect and storage) and intercluster peering.

Failure scenarios during which Tiebreaker software triggers an alert

The Tiebreaker software triggers an alert when the cluster (all of the nodes) at the disaster site is down or unreachable and the cluster at the surviving site indicates the “AllLinksSevered” status.

The Tiebreaker software does not trigger an alert (or the alert is vetoed) in the following scenarios:

- In an eight-node MetroCluster configuration, if one HA pair at the disaster site is down
- In a cluster with all of the nodes at the disaster site down, one HA pair at the surviving site down, and the cluster at the surviving site indicates the “AllLinksSevered” status

  The Tiebreaker software triggers an alert, but ONTAP vetoes that alert. In this situation, a manual switchover is also vetoed

- Any scenario in which the Tiebreaker software can either reach at least one node or the cluster interface at the disaster site, or the surviving site still can reach either node at the disaster site through either FC (NV interconnect and storage) or intercluster peering

Related information

Risks and limitations of using MetroCluster Tiebreaker in active mode

How the Tiebreaker software detects intersite connectivity failures

The MetroCluster Tiebreaker software alerts you if all connectivity between the sites is lost.

Types of network paths

Depending on the configuration, there are three types of network paths between the two clusters in a MetroCluster configuration:

- **FC network (present in fabric-attached MetroCluster configurations)**

  This type of network is composed of two redundant FC switch fabrics. Each switch fabric has two FC switches, with one switch of each switch fabric co-located with a cluster. Each cluster has two FC switches, one from each switch fabric. All of the nodes have FC (NV interconnect and FCP initiator) connectivity to each of the co-located FC switches. Data is replicated from cluster to cluster over the ISL.

- **Intercluster peering network**

  This type of network is composed of a redundant IP network path between the two clusters. The cluster peering network provides the connectivity that is required to mirror the storage virtual machine (SVM) configuration. The configuration of all of the SVMs on one cluster is mirrored by the partner cluster.

- **IP network (present in MetroCluster IP configurations)**

  This type of network is composed of two redundant IP switch networks. Each network has two IP switches, with one switch of each switch fabric co-located with a cluster. Each cluster has two IP switches, one from each switch fabric. All of the nodes have connectivity to each of the co-located FC switches. Data is replicated from cluster to cluster over the ISL.

Monitoring intersite connectivity

The Tiebreaker software regularly retrieves the status of intersite connectivity from the nodes. If NV interconnect connectivity is lost and the intercluster peering does not respond to pings, then the clusters assume that the sites are isolated and the Tiebreaker software triggers an alert as “AllLinksSevered”. If a cluster identifies the “AllLinksSevered” status and the other cluster is not reachable through the network, then the Tiebreaker software triggers an alert as “disaster”.

How different disaster types affect Tiebreaker software detection time

For better disaster recovery planning, the MetroCluster Tiebreaker software takes some time in detecting a disaster. This time spent is the “disaster detection time”. The MetroCluster Tiebreaker software detects the site disaster within 30 seconds from the time of occurrence of the disaster and triggers the disaster recovery operation to notify you about the disaster.

The detection time also depends on the type of disaster and might exceed 30 seconds in some scenarios, mostly known as “rolling disasters”. The main types of rolling disaster are as follows:

- Power loss
- Panic
- Halt or reboot
- Loss of FC switches at the disaster site

Power loss

The Tiebreaker software immediately triggers an alert when the node stops operating. When there is a power loss, all connections and updates, such as intercluster peering, NV interconnect, and MailBox disk, stop. The time taken between the cluster becoming unreachable, the detection of the disaster, and the trigger, including the default silent time of 5 seconds, should not exceed 30 seconds.

Panic

The Tiebreaker software triggers an alert when the NV interconnect connection between the sites is down and the surviving site indicates the “AllLinksSevered” status. This only happens after the coredump process is complete. In this scenario, the time taken between the cluster becoming unreachable and the detection of a disaster might be longer or approximately equal to the time taken for the coredump process. In many cases, the detection time is more than 30 seconds.

If a node stops operating but does not generate a file for the coredump process, then the detection time should not be longer than 30 seconds.

Halt or reboot

The Tiebreaker software triggers an alert only when the node is down and the surviving site indicates the “AllLinksSevered” status. The time taken between the cluster becoming unreachable and the detection of a disaster might be longer than 30 seconds. In this scenario, the time taken to detect a disaster depends on how long it takes for the nodes at the disaster site to be shut down.

Loss of FC switches at the disaster site (fabric-attached MetroCluster configuration)

The Tiebreaker software triggers an alert when a node stops operating. If FC switches are lost, then the node tries to recover the path to a disk for about 30 seconds. During this time, the node is up and responding on the peering network. When both of the FC switches are down and the path to a disk cannot be recovered, the node produces a MultiDiskFailure error and halts. The time taken between the FC switch failure and the number of times the nodes produced MultiDiskFailure errors is about 30 seconds longer. This additional 30 seconds must be added to the disaster detection time.

About the Tiebreaker CLI and man pages

The Tiebreaker CLI provides commands that enable you to remotely configure the Tiebreaker software and monitor the MetroCluster configurations.

The CLI command prompt is represented as NetApp MetroCluster Tiebreaker::>.

The man pages are available in the CLI by entering the applicable command name at the prompt.

Installing the Tiebreaker software

The Tiebreaker software provides monitoring capabilities for a clustered storage environment. It also sends SNMP notifications in the event of node connectivity issues and site disasters.

The MetroCluster software must be installed and configured.

System requirements for installing or upgrading Tiebreaker software

The Tiebreaker software is installed on a third site, which allows the software to distinguish between an Inter-Switch Link (ISL) failure (when inter-site links are down) and a site failure. Your host system must meet certain requirements before you can install or upgrade the Tiebreaker software on your local computer to monitor the MetroCluster configuration.

The MetroCluster Tiebreaker software has the following monitoring capabilities and requirements:

- No requirement for a special configuration for the different MetroCluster configurations.
- Monitoring capabilities for up to 15 MetroCluster configurations simultaneously.

  > You should have only one MetroCluster Tiebreaker monitor per MetroCluster configuration to avoid any conflict with multiple Tiebreaker monitors.

- Support for a combination of MetroCluster IP, MetroCluster FC, and stretch MetroCluster configurations.
- Hardware and software:
  - ONTAP 8.3.x, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7 and 9.8
- Red Hat Enterprise Linux 7 to 7.6 or CentOS 7 to 7.6 64-bit (physical installation or virtual machine)
  - MariaDB 5.5.52.x
  - 4 GB RAM

    - Open Java Runtime Environment 8
- Red Hat Enterprise Linux 6.4 to 6.10 or CentOS 6.4 to 6.10 64-bit (physical installation or virtual machine)
    - MySQL Server 5.6.x
    - 2 GB RAM
    - Open Java Runtime Environment 8
- Disk capacity: 8 GB
- User: Root access
- Firewall:
    - Direct access for setting up AutoSupport messages
    - SSH (port 22/TCP), HTTPS (port 443/TCP), and ping (ICMP)
- Installation on FIPS-enabled hosts is not supported.

Installing MetroCluster Tiebreaker dependencies

You must install a MySQL or MariaDB server depending on the Linux operating system that is your host before installing or upgrading the Tiebreaker software.

Steps

1. Install Java Runtime Environment.

   Installing Java Runtime Environment 1.8

2. Install MySQL or MariaDB server:

If the Linux host is	Then…
Red Hat Enterprise Linux 6/CentOS 6	a. Install MySQL Installing MySQL Server 5.5.30 or later and 5.6.x versions on Red Hat Enterprise Linux 6 or CentOS 6
Red Hat Enterprise Linux 7/CentOS 7	a. Install MariaDB Installing MariaDB server on Red Hat Enterprise Linux 7 or CentOS 7

Installing Java Runtime Environment 1.8

You must install Java Runtime Environment 1.8 on your host system before installing or upgrading the Tiebreaker software.

Steps

1. Log in as `root` to the host system.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Install Java Runtime Environment 1.8: `[root@mcctb ~]# yum install java-1.8.0-openjdk.x86_64`

```
[root@mcctb ~]# yum install java-1.8.0-openjdk.x86_64
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
... shortened....
Dependencies Resolved

========================================================================
=======================
Package                Arch   Version                     Repository
Size
========================================================================
=======================
Installing:
 java-1.8.0-openjdk  x86_64  1:1.8.0.144-0.b01.el7_4      updates
238 k
 ..
 ..
Transaction Summary
========================================================================
========================
Install  1 Package  (+ 4 Dependent packages)

Total download size: 34 M
Is this ok [y/d/N]: y

Installed:
java-1.8.0-openjdk.x86_64 1:1.8.0.144-0.b01.el7_4
Complete!
```

Installing MySQL Server 5.5.30 or later and 5.6.x versions on Red Hat Enterprise Linux 6 or CentOS 6

You must install MySQL Server 5.5.30 or later and 5.6.x version on your host system before installing or upgrading the Tiebreaker software.

Steps

1. Log in as `root` to the host system.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2016 from host.domain.com
```

2. Add the MySQL repository to your host system: `[root@mcctb ~]# yum localinstall https://dev.mysql.com/get/mysql57-community-release-el6-11.noarch.rpm`

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
Setting up Local Package Process
Examining /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm: mysql-community-release-el6-5.noarch
Marking /var/tmp/yum-root-LLUw0r/mysql-community-release-el6-
5.noarch.rpm to be installed
Resolving Dependencies
--> Running transaction check
---> Package mysql-community-release.noarch 0:el6-5 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
========================================================================
========
Package               Arch   Version
                                    Repository
Size
========================================================================
========
Installing:
mysql-community-release
                       noarch el6-5 /mysql-community-release-el6-
5.noarch 4.3 k
Transaction Summary
========================================================================
========
Install       1 Package(s)
Total size: 4.3 k
Installed size: 4.3 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-release-el6-5.noarch
1/1
  Verifying  : mysql-community-release-el6-5.noarch
1/1
Installed:
  mysql-community-release.noarch 0:el6-5
Complete!
```

3. Disable the mysql 57 repository: `[root@mcctb ~]# yum-config-manager --disable mysql57-community`

4. Enable the mysql 56 repository: `[root@mcctb ~]# yum-config-manager --enable mysql56-community`
5. Enable the repository: `[root@mcctb ~]# yum repolist enabled | grep "mysql.`**`-community.`**`"`

```
mysql-connectors-community           MySQL Connectors Community
21
mysql-tools-community                MySQL Tools Community
35
mysql56-community                    MySQL 5.6 Community Server
231
```

6. Install the MySQL Community server: `[root@mcctb ~]# yum install mysql-community-server`

```
Loaded plugins: product-id, refresh-packagekit, security, subscription-
manager
This system is not registered to Red Hat Subscription Management. You
can use subscription-manager
to register.
Setting up Install Process
Resolving Dependencies
--> Running transaction check
....Output truncated....
---> Package mysql-community-libs-compat.x86_64 0:5.6.29-2.el6 will be
obsoleting
--> Finished Dependency Resolution
Dependencies Resolved
========================================================================
==========================
Package                                    Arch         Version
Repository         Size
========================================================================
==========================
Installing:
 mysql-community-client                     x86_64      5.6.29-2.el6
mysql56-community  18  M
     replacing  mysql.x86_64 5.1.71-1.el6
 mysql-community-libs                       x86_64      5.6.29-2.el6
mysql56-community  1.9 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-libs-compat                x86_64      5.6.29-2.el6
mysql56-community  1.6 M
     replacing  mysql-libs.x86_64 5.1.71-1.el6
 mysql-community-server                     x86_64      5.6.29-2.el6
mysql56-community  53  M
```

```
     replacing  mysql-server.x86_64 5.1.71-1.el6
Installing for dependencies:
mysql-community-common                            x86_64       5.6.29-2.el6
mysql56-community   308 k

Transaction Summary
================================================================================
==========================
Install       5 Package(s)
Total download size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/5): mysql-community-client-5.6.29-2.el6.x86_64.rpm
|  18 MB     00:28
(2/5): mysql-community-common-5.6.29-2.el6.x86_64.rpm
| 308 kB     00:01
(3/5): mysql-community-libs-5.6.29-2.el6.x86_64.rpm
| 1.9 MB     00:05
(4/5): mysql-community-libs-compat-5.6.29-2.el6.x86_64.rpm
| 1.6 MB     00:05
(5/5): mysql-community-server-5.6.29-2.el6.x86_64.rpm
|  53 MB     03:42
--------------------------------------------------------------------------------
--------------------------
Total
289 kB/s |  74 MB     04:24
warning: rpmts_HdrFromFdno: Header V3 DSA/SHA1 Signature, key ID
5072e1f5: NOKEY
Retrieving key from file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Importing GPG key 0x5072E1F5:
 Userid : MySQL Release Engineering <mysql-build@oss.oracle.com>
Package: mysql-community-release-el6-5.noarch (@/mysql-community-
release-el6-5.noarch)
 From   : file:/etc/pki/rpm-gpg/RPM-GPG-KEY-mysql
Is this ok [y/N]: y
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : mysql-community-common-5.6.29-2.el6.x86_64
....Output truncated....
1.el6.x86_64
7/8
  Verifying  : mysql-5.1.71-1.el6.x86_64
8/8
Installed:
```

```
  mysql-community-client.x86_64 0:5.6.29-2.el6          mysql-community-
libs.x86_64 0:5.6.29-2.el6
  mysql-community-libs-compat.x86_64 0:5.6.29-2.el6   mysql-community-
server.x86_64 0:5.6.29-2.el6

Dependency Installed:
  mysql-community-common.x86_64 0:5.6.29-2.el6

Replaced:
  mysql.x86_64 0:5.1.71-1.el6 mysql-libs.x86_64 0:5.1.71-1.el6  mysql-
server.x86_64 0:5.1.71-1.el6
Complete!
```

7. Start MySQL server: `[root@mcctb ~]# service mysqld start`

```
Initializing MySQL database:  2016-04-05 19:44:38 0 [Warning] TIMESTAMP
with implicit DEFAULT
value is deprecated. Please use --explicit_defaults_for_timestamp server
option (see documentation
 for more details).
2016-04-05 19:44:38 0 [Note] /usr/sbin/mysqld (mysqld 5.6.29) starting
as process 2487 ...
2016-04-05 19:44:38 2487 [Note] InnoDB: Using atomics to ref count
buffer pool pages
2016-04-05 19:44:38 2487 [Note] InnoDB: The InnoDB memory heap is
disabled
....Output truncated....
2016-04-05 19:44:42 2509 [Note] InnoDB: Shutdown completed; log sequence
number 1625987

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER!
To do so, start the server, then issue the following commands:

  /usr/bin/mysqladmin -u root password 'new-password'
  /usr/bin/mysqladmin -u root -h mcctb password 'new-password'

Alternatively, you can run:
  /usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.
....Output truncated....
WARNING: Default config file /etc/my.cnf exists on the system
This file will be read by default by the MySQL server
If you do not want to use this, either remove it, or use the
--defaults-file argument to mysqld_safe when starting the server

                                                           [  OK  ]
Starting mysqld:                                           [  OK  ]
```

8. Confirm that MySQL server is running: `[root@mcctb ~]# service mysqld status`

```
mysqld (pid  2739) is running...
```

9. Configure security and password settings: `[root@mcctb ~]# mysql_secure_installation`

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
       SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!
```

```
 In order to log into MySQL to secure it, we'll need the current
 password for the root user.  If you've just installed MySQL, and
 you haven't set the root password yet, the password will be blank,
 so you should just press enter here.

 Enter current password for root (enter for none):   <== on default
install hit enter here
 OK, successfully used password, moving on...

 Setting the root password ensures that nobody can log into the MySQL
 root user without the proper authorisation.

 Set root password? [Y/n] y
 New password:
 Re-enter new password:
 Password updated successfully!
 Reloading privilege tables..
  ... Success!

 By default, a MySQL installation has an anonymous user, allowing anyone
 to log into MySQL without having to have a user account created for
 them.  This is intended only for testing, and to make the installation
 go a bit smoother.  You should remove them before moving into a
 production environment.

 Remove anonymous users? [Y/n] y
  ... Success!

 Normally, root should only be allowed to connect from 'localhost'.
This
 ensures that someone cannot guess at the root password from the
network.

 Disallow root login remotely? [Y/n] y
  ... Success!

 By default, MySQL comes with a database named 'test' that anyone can
 access.  This is also intended only for testing, and should be removed
 before moving into a production environment.

 Remove test database and access to it? [Y/n] y
  - Dropping test database...
 ERROR 1008 (HY000) at line 1: Can't drop database 'test'; database
doesn't exist
  ... Failed!  Not critical, keep moving...
```

```
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
 ... Success!

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!

Cleaning up...
```

10. Verify that the MySQL login is working: `[root@mcctb ~]# mysql -u root -p`

```
Enter password: <configured_password>
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 17
Server version: 5.6.29 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights
reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.
mysql>
```

If the MySQL login is working, the output will end at the `mysql>` prompt.

Enabling the MySQL autostart setting

You should ensure that the autostart feature is turned on for the MySQL deamon. Turning on the MySQL daemon automatically restarts MySQL if the system on which the MetroCluster Tiebreaker software resides reboots. If the MySQL daemon is not running, the Tiebreaker software continues running, but it cannot be restarted and configuration changes cannot be made.

See the MySQL documentation to enable autostart on your installation.

Installing MariaDB server on Red Hat Enterprise Linux 7 or CentOS 7

You must install MariaDB server on your host system before installing or upgrading the Tiebreaker software.

Your host system must be running on Red Hat Enterprise Linux (RHEL) 7 or CentOS 7.

Steps

1. Log in as `root` to the host system.

```
login as: root
root@mcctb's password:
Last login: Fri Jan  8 21:33:00 2017 from host.domain.com
```

2. Install MariaDB server: `[root@mcctb ~]# yum install mariadb-server.x86_64`

```
 [root@mcctb ~]# yum install mariadb-server.x86_64
Loaded plugins: fastestmirror, langpacks
...
...

========================================================================
===============
 Package                         Arch    Version         Repository
Size
========================================================================
===============
Installing:
mariadb-server                  x86_64   1:5.5.56-2.el7   base
11 M
Installing for dependencies:

Transaction Summary
========================================================================
===============
Install  1 Package  (+8 Dependent packages)
Upgrade             ( 1 Dependent package)

Total download size: 22 M
Is this ok [y/d/N]: y
Downloading packages:
No Presto metadata available for base
warning: /var/cache/yum/x86_64/7/base/packages/mariadb-libs-5.5.56-
2.el7.x86_64.rpm:
Header V3 RSA/SHA256 Signature, key ID f4a80eb5: NOKEY] 1.4 MB/s | 3.3
MB  00:00:13 ETA
```

```
Public key for mariadb-libs-5.5.56-2.el7.x86_64.rpm is not installed
(1/10): mariadb-libs-5.5.56-2.el7.x86_64.rpm  | 757 kB  00:00:01
..
..
(10/10): perl-Net-Daemon-0.48-5.el7.noarch.rpm|  51 kB  00:00:01
------------------------------------------------------------------------
-----------------
Installed:
  mariadb-server.x86_64 1:5.5.56-2.el7

Dependency Installed:
mariadb.x86_64 1:5.5.56-2.el7         perl-Compress-Raw-Bzip2.x86_64
0:2.061-3.el7
perl-Compress-Raw-Zlib.x86_64 1:2.061-4.el7 perl-DBD-MySQL.x86_64
0:4.023-5.el7
perl-DBI.x86_64 0:1.627-4.el7  perl-IO-Compress.noarch 0:2.061-2.el7
perl-Net-Daemon.noarch 0:0.48-5.el7          perl-PlRPC.noarch 0:0.2020-
14.el7

Dependency Updated:
  mariadb-libs.x86_64 1:5.5.56-2.el7
Complete!
```

3. Start MariaDB server: `[root@mcctb ~]# systemctl start mariadb`

```
[root@mcctb ~]# systemctl start mariadb
```

4. Verify MariaDB server has started: `[root@mcctb ~]# systemctl status mariadb`

```
[root@mcctb ~]# systemctl status mariadb
mariadb.service - MariaDB database server
...
Nov 08 21:28:59 mcctb systemd[1]: Starting MariaDB database server...
...
Nov 08 21:29:01 scspr0523972001 systemd[1]: Started MariaDB database
server.
```

Ensure that the enable autostart setting is turned on for MariaDB.

5. Configure the security and password settings: `[root@mcctb ~]# mysql_secure_installation`

```
[root@mcctb ~]# mysql_secure_installation
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
Set root password? [Y/n] y
New password:
Re-enter new password:
Password updated successfully!
Remove anonymous users? [Y/n] y
... Success!
Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.
Disallow root login remotely? [Y/n] y
... Success!
Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!
Reload privilege tables now? [Y/n]
... Success!
Cleaning up...
All done! If you've completed all of the above steps, your MariaDB
installation should now be secure.
Thanks for using MariaDB!
```

Installing or upgrading the software package

You must install or upgrade the MetroCluster Tiebreaker software on your local computer to monitor MetroCluster configurations.

- Your storage system must be running ONTAP 8.3.x or later.
- You must have installed OpenJDK by using the yum install java-1.8.0-openjdk command.

Steps

1. Download the NetApp-MetroCluster-Tiebreaker-Software-1.21P3-1.x86_64.rpm file.

   NetApp Support

2. Log in to the host as the root user.
3. Install or upgrade the Tiebreaker software:

<table>
<tr><th>If you are…</th><th>Issue this command…</th></tr>
<tr><td>Performing a new installation</td><td>rpm -ivh NetApp-MetroCluster-Tiebreaker-Software-1.21P3-1.x86_64.rpm

The system displays the following output for a successful installation:

<pre>
[root@scspr0523972001 mcctb]# rpm
-ivh NetApp-MetroCluster-
Tiebreaker-Software-1.21P3-
1.x86_64.rpm
Preparing...
#################################
[100%]
Updating / installing...
   1:NetApp-MetroCluster-
Tiebreaker-
So#################################
[100%]
Post installation start Wed Sep
5 05:56:18 EDT 2018
Enter MetroCluster Tiebreaker
user password:

Please enter mysql root password
when prompted
Enter password:
Created symlink from
/etc/systemd/system/multi-
user.target.wants/netapp-
metrocluster-tiebreaker-
software.service to
/etc/systemd/system/netapp-
metrocluster-tiebreaker-
software.service.
Enabled autostart of NetApp
MetroCluster Tiebreaker software
daemon during boot
Created symbolic link for NetApp
MetroCluster Tiebreaker software
CLI
Post installation end Wed Sep 5
05:56:24 EDT 2018
Successfully installed NetApp
MetroCluster Tiebreaker software
version 1.21P3
</pre>
</td></tr>
</table>

If you are…	Issue this command…

Upgrading an existing installation	rpm -Uvh NetApp-MetroCluster-Tiebreaker-Software-1.21P3-1.x86_64.rpm
	
	The system displays the following output for a successful upgrade:
	
	<pre>[root@scspr0523972001 mcctb]# rpm
	-Uvh NetApp-MetroCluster-
	Tiebreaker-Software-1.21P3-
	1.x86_64.rpm
	Preparing...
	#################################
	[100%]
	Upgrading NetApp MetroCluster
	Tiebreaker software....
	Stopping NetApp MetroCluster
	Tiebreaker software services
	before upgrade.
	Stopping NetApp MetroCluster
	Tiebreaker software daemon [
	OK]
	Updating / installing...
	   1:NetApp-MetroCluster-
	Tiebreaker-
	So###############################
	## [50%]
	Post installation start Wed Sep
	5 05:59:13 EDT 2018
	Enabled autostart of NetApp
	MetroCluster Tiebreaker software
	daemon during boot
	Created symbolic link for NetApp
	MetroCluster Tiebreaker software
	CLI
	Post installation end Wed Sep 5
	05:59:13 EDT 2018
	Successfully installed NetApp
	MetroCluster Tiebreaker software
	version 1.21P3
	Cleaning up / removing...
	   2:NetApp-MetroCluster-
	Tiebreaker-
	So###############################
	## [100%]</pre>

If you enter the wrong MySQL root password, the Tiebreaker software indicates that it was installed successfully, but displays Access denied messages. To resolve the issue, you must uninstall the Tiebreaker software by using the rpm -e command, and then reinstall the software by using the correct MySQL root password.

Steps

1. Verify the Tiebreaker connectivity to the MetroCluster software by opening an SSH connection from the Tiebreaker host to each of the node management LIFs and cluster management LIFs.

Related information

NetApp Support

Upgrading the host where the Tiebreaker monitor is running

You can upgrade the host where the Tiebreaker monitor is running with minimal disruption if you place the monitors in observer mode before the upgrade.

Steps

1. Verify the monitors are in observer mode: `monitor show -status`

```
NetApp MetroCluster Tiebreaker:> monitor show -status
MetroCluster: cluster_A
    Disaster: false
    Monitor State: Normal
    Observer Mode: true
    Silent Period: 15
    Override Vetoes: false
    Cluster: cluster_Ba(UUID:4d9ccf24-080f-11e4-9df2-00a098168e7c)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-a1(UUID:78b44707-0809-11e4-9be1-e50dab9e83e1)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-a2(UUID:9a8b1059-0809-11e4-9f5e-8d97cdec7102)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
    Cluster: cluster_B(UUID:70dacd3b-0823-11e4-a7b9-00a0981693c4)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-b1(UUID:961fce7d-081d-11e4-9ebf-2f295df8fcb3)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-b2(UUID:9393262d-081d-11e4-80d5-6b30884058dc)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
```

2. Change all of the monitors to observer mode.

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name
monitor_name -observer-mode true
```

3. To upgrade the Tiebreaker host, follow all of the steps in the following procedure:

   Installing or upgrading the software package

4. Disable observer mode to move all the of the monitors back to online mode.

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name
monitor_name -observer-mode false
```

Selecting the NTP source for the Tiebreaker software

You should use a local Network Time Protocol (NTP) source for the Tiebreaker software. It should not use the same source as the MetroCluster sites that the Tiebreaker software monitors.

Configuring the Tiebreaker software

After installation of the Tiebreaker software, you can add or modify MetroCluster configurations, or remove them from the Tiebreaker software.

Launching the Tiebreaker software CLI

After installing the Tiebreaker software you must launch its CLI to configure the software.

1. Launch the CLI from the prompt of the host on which you installed the software:`netapp-metrocluster-tiebreaker-software-cli`

Adding MetroCluster configurations

After installing the NetApp MetroCluster Tiebreaker software, you can add more MetroCluster configurations, one at a time.

You must have installed the MetroCluster configuration in an ONTAP environment and enabled the settings in the software.

1. Use the Tiebreaker command-line interface (CLI) monitor add command to add MetroCluster configurations.

   If you are using the host name, it must be the fully qualified domain name (FQDN).

   The following example shows the configuration of cluster_A:

   ```
   NetApp MetroCluster Tiebreaker :> monitor add wizard
   Enter monitor Name: cluster_A
   Enter Cluster IP Address: 10.222.196.130
   Enter Cluster Username: admin
   Enter Cluster Password:
   Enter Peer Cluster IP Address: 10.222.196.40
   Enter Peer Cluster Username: admin
   Enter Peer Cluster Password:
   Successfully added monitor to NetApp MetroCluster Tiebreaker software.
   ```

2. Confirm that the MetroCluster configuration was added properly by using the Tiebreaker CLI monitor show -status command.

   ```
   NetApp MetroCluster Tiebreaker :> monitor show -status
   ```

3. Disable the observer mode for the Tiebreaker software to automatically initiate a switchover after it detects a site failure: `monitor modify -monitor-name monitor_name -observer-mode false`

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name 8pack
-observer-mode false
Warning: If you are turning observer-mode to false, make sure to review
the 'risks and limitations'
as described in the MetroCluster Tiebreaker Installation and
Configuration Guide.
Are you sure you want to enable automatic switchover capability for
monitor "8pack"? [Y/N]: y
```

Related information

Risks and limitations of using MetroCluster Tiebreaker in active mode

Commands for modifying MetroCluster Tiebreaker configurations

You can modify the MetroCluster configuration whenever you need to change the settings.

The Tiebreaker CLI monitor modify command can be used with any of the following options. You can confirm your changes with the monitor show -status command.

Option	Description
-monitor-name	Name of the MetroCluster configuration
-enable-monitor	Enables and disables monitoring of the MetroCluster configuration
-silent-period	Period in seconds for which the MetroCluster Tiebreaker software waits to confirm a site failure after detection
-observer-mode	Observer mode (true) provides monitoring only, and does not trigger a switchover if a site disaster occurs. Online mode (false) triggers a switchover if a site disaster occurs. • How the Tiebreaker software detects site failure • Risks and limitations of using MetroCluster Tiebreaker in active mode

The following example changes the silent period for the configuration.

```
NetApp MetroCluster Tiebreaker :> monitor modify -monitor-name cluster_A
-silent-period 15
Successfully modified monitor in NetApp MetroCluster Tiebreaker
software.
```

The Tiebreaker CLI debug command can be used to change the logging mode.

Command	Description
debug status	Displays the status of the debug mode
debug enable	Enables the debug mode for logging
debug disable	Disables the debug mode for logging

The Tiebreaker CLI update-mcctb-password command can be used to update the user password.

Command	Description
update-mcctb-password	The user password is successfully updated

Removing MetroCluster configurations

You can remove the MetroCluster configuration that is being monitored by the Tiebreaker software when you no longer want to monitor a MetroCluster configuration.

1. Use the Tiebreaker CLI monitor remove command to remove the MetroCluster configuration.

   In the following example, cluster_A is removed from the software:

   ```
   NetApp MetroCluster Tiebreaker :> monitor remove -monitor-name cluster_A
   Successfully removed monitor from NetApp MetroCluster Tiebreaker
   software.
   ```

2. Confirm that the MetroCluster configuration is removed properly by using the Tiebreaker CLI monitor show -status command.

   ```
   NetApp MetroCluster Tiebreaker :> monitor show -status
   ```

Configuring SNMP settings for Tiebreaker software

To use SNMP with the Tiebreaker software, you must configure SNMP settings.

1. Use the Tiebreaker CLI snmp config wizard command to add MetroCluster configurations.

   The following example shows the configuration of an SNMP receiver that supports SNMP V1 with an IP address of 10.222.210.234, port number 162 for trap messages, and the community string set to public:

   ```
   NetApp MetroCluster Tiebreaker :> snmp config wizard
   Enter SNMP Version [V1/V3]: V1
   Enter SNMP Host: 10.222.210.234
   Enter SNMP Port: 162
   Enter SNMP V1 Community: public
   Successfully added SNMP properties to NetApp MetroCluster Tiebreaker
   software.
   NetApp MetroCluster Tiebreaker :>
   ```

   The Tiebreaker software is ready to send traps to the SNMP receiver that you specified.

2. Verify that the SNMP settings are configured: `snmp config test`

   The following example shows that the Tiebreaker software can send an SNMP trap for the event TEST_SNMP_CONFIG:

   ```
   NetApp MetroCluster Tiebreaker :> snmp config test
   Sending SNMP trap to localhost. Version : V1.
   Successfully sent SNMP trap for event TEST_SNMP_CONFIG
   NetApp MetroCluster Tiebreaker :>
   ```

Monitoring the MetroCluster configuration

MetroCluster Tiebreaker software automates the recovery process by enabling you to monitor the MetroCluster configuration status, evaluate SNMP events and traps that are sent to NetApp customer support, and view the status of monitoring operations.

Configuring AutoSupport

By default, AutoSupport messages are sent to NetApp a week after installation of the Tiebreaker software. Events that trigger AutoSupport notification include Tiebreaker software panics, detection of disaster conditions on MetroCluster configurations, or an unknown MetroCluster configuration status.

You must have a direct access for setting up AutoSupport messages.

1. Use the Tiebreaker CLI autosupport command with any of the following options:

Option	Description
-invoke	Sends an AutoSupport message to customer support
-configure wizard	Wizard to configure proxy server credentials
-delete configuration	Deletes the proxy server credentials
--enable	Enables AutoSupport notification (This is the default.)
-disable	Disables AutoSupport notification
-show	Displays AutoSupport status

The following example shows that AutoSupport is enabled or disabled and the destination to which the AutoSupport content is posted:

```
NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport already enabled.

NetApp MetroCluster Tiebreaker :> autosupport disable
AutoSupport status             : disabled
Proxy Server IP Address        : 10.234.168.79
Proxy Server Port Number       : 8090
Proxy Server Username          : admin
AutoSupport destination        :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport enable
AutoSupport status             : enabled
Proxy Server IP Address        : 10.234.168.79
Proxy Server Port Number       : 8090
Proxy Server Username          : admin
AutoSupport destination        :
https://support.netapp.com/asupprod/post/1.0/postAsup

NetApp MetroCluster Tiebreaker :> autosupport invoke
AutoSupport transmission       : success
Proxy Server IP Address        : 10.234.168.79
Proxy Server Port Number       : 8090
Proxy Server Username          : admin
AutoSupport destination        :
https://support.netapp.com/asupprod/post/1.0/postAsup
```

The following example shows AutoSupport configured by means of an authenticated proxy server, using an IP address and port number:

```
NetApp MetroCluster Tiebreaker :> autosupport configure wizard
Enter Proxy Server IP address :  10.234.168.79
Enter Proxy Server port number :  8090
Enter Proxy Server Username :  admin
Enter Proxy Server Password : 123abc
Autosupport configuration updated successfully.
```

The following example shows the deletion of an AutoSupport configuration:

```
NetApp MetroCluster Tiebreaker :> autosupport delete configuration
Autosupport configuration deleted successfully.
```

SNMP events and traps

NetApp MetroCluster Tiebreaker software uses SNMP traps to notify you of significant events. These traps are part of the NetApp MIB file. Each trap contains the following information: trap name, severity, impact level, timestamp, and message.

Event name	Event detail	Trap number
MetroCluster Tie-Breaker is unable to reach the MetroCluster configuration	Warns the administrator that the software cannot detect a disaster. This event occurs when both clusters are not reachable.	25000
MetroCluster Tie-Breaker is unable to reach cluster	Warns the administrator that the software cannot reach one of the clusters.	25001
MetroCluster Tie-Breaker detected disaster at cluster	Notifies the administrator that the software detects a site failure. A notification will be delivered.	25002
All links between partner cluster are severed.	The software detects that both clusters are reachable, but all the network paths between the two clusters are down, and the clusters cannot communicate with each other.	25005
SNMP Test Trap	SNMP configuration can now be tested by running the snmp config test command.	25006

Displaying the status of monitoring operations

You can display the overall status of monitoring operations for a MetroCluster configuration.

1. Use the Tiebreaker CLI monitor show command to display the status of a MetroCluster operation with any of the following options:

Option	Description
-monitor-name	Displays the status for the specified monitor name
-operation-history	Displays up to 10 monitoring operations that were last performed on a cluster
-stats	Displays the statistics related to the specified cluster
-status	Displays the status of the specified cluster **Note:** The MetroCluster Tiebreaker software might take up to 10 minutes to reflect the completion status of operations such as heal aggregates, heal roots, or switchback.

The following example shows that the clusters cluster_A and cluster_B are connected and healthy:

```
NetApp MetroCluster Tiebreaker:> monitor show -status
MetroCluster: cluster_A
    Disaster: false
    Monitor State: Normal
    Observer Mode: true
    Silent Period: 15
    Override Vetoes: false
    Cluster: cluster_Ba(UUID:4d9ccf24-080f-11e4-9df2-00a098168e7c)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-a1(UUID:78b44707-0809-11e4-9be1-e50dab9e83e1)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-a2(UUID:9a8b1059-0809-11e4-9f5e-8d97cdec7102)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
    Cluster: cluster_B(UUID:70dacd3b-0823-11e4-a7b9-00a0981693c4)
        Reachable: true
        All-Links-Severed: FALSE
            Node: mcc5-b1(UUID:961fce7d-081d-11e4-9ebf-2f295df8fcb3)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
            Node: mcc5-b2(UUID:9393262d-081d-11e4-80d5-6b30884058dc)
                Reachable: true
                All-Links-Severed: FALSE
                State: normal
```

In the following example, the last seven operations that were run on cluster_B are displayed:

```
NetApp MetroCluster Tiebreaker:> monitor show -operation-history
MetroCluster: cluster_B
 [ 2014-09-15 04:48:32.274 ] MetroCluster Monitor is initialized
 [ 2014-09-15 04:48:32.278 ] Started Discovery and validation of
MetroCluster Setup
 [ 2014-09-15 04:48:35.078 ] Discovery and validation of MetroCluster
Setup succeeded. Started monitoring.
 [ 2014-09-15 04:48:35.246 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5a"
 [ 2014-09-15 04:48:35.256 ] NetApp MetroCluster Tiebreaker software is
able to reach cluster "mcc5b"
 [ 2014-09-15 04:48:35.298 ] Link to remote DR cluster is up for cluster
"mcc5a"
 [ 2014-09-15 04:48:35.308 ] Link to remote DR cluster is up for cluster
"mcc5b"
```

Displaying MetroCluster configuration information

You can display the monitor name and IP address of all instances of MetroCluster configurations in the Tiebreaker software.

1. Use the Tiebreaker CLI configuration show command to display the MetroCluster configuration information.

   The following example shows the information for clusters cluster_A and cluster_B:

```
MetroCluster: North America
    Monitor Enabled: true
    ClusterA name: cluster_A
    ClusterA IpAddress: 10.222.196.130
    ClusterB name: cluster_B
    ClusterB IpAddress: 10.222.196.140
```

Creating dump files

You save the overall status the Tiebreaker software to a dump file for debugging purposes.

1. Use the Tiebreaker CLI monitor dump -status command to create a dump file of the overall status of all MetroCluster configurations.

   The following example shows the successful creation of the /var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml dump file:

```
NetApp MetroCluster Tiebreaker :> monitor dump -status
MetroCluster Tiebreaker status successfully dumped in file
/var/log/netapp/mcctb/metrocluster-tiebreaker-status.xml
```

Risks and limitations of using MetroCluster Tiebreaker in active mode

Switchover upon detection of a site failure happens automatically, with MetroCluster Tiebreaker in active mode. This mode can be used to supplement the ONTAP/FAS automatic switchover capability.

When you implement MetroCluster Tiebreaker in active mode, the following known issues might lead to data loss:

- When the inter-site link fails, the controllers on each site continue to serve the clients. However, the controllers will not be mirrored. Failure of a controller in one site is identified as a site failure and the MetroCluster Tiebreaker initiates a switchover. The data which is not mirrored after the inter-site link failure with the remote site will be lost.
- A switchover occurs when the aggregates in remote site are in degraded state. The data will not be replicated if the switchover has occurred before aggregate resync.
- A remote storage failure occurs when switchover is in progress.
- The nonvolatile memory (NVRAM or NVMEM, depending on the platform model) in the storage controllers is not mirrored to the remote disaster recovery (DR) partner on the partner site.
- Metadata is lost if the cluster peering network is down for an extended period and the metadata volumes are not online after a switchover.

> You might encounter scenarios that are not mentioned. NetApp is not responsible for any damages that may arise out of use of MetroCluster Tiebreaker in active mode. Do not use MetroCluster Tiebreaker in active mode if the risks and limitations are not acceptable to you.

Firewall requirements for MetroCluster Tiebreaker

MetroCluster Tiebreaker uses a number of ports to communicate with specific services.

The following table lists the ports that you must allow in your firewall:

Port/services	Source	Destination	Purpose
443 / TCP	Tiebreaker	Internet	Sending AutoSupport messages to NetApp
22 / TCP	Management host	Tiebreaker	Tiebreaker Management
443 / TCP	Tiebreaker	MetroCluster management LIFs	Secure communications via HTTP (SSL)

Port/services	Source	Destination	Purpose
22 / TCP	Tiebreaker	MetroCluster management LIFs	Secure communications via SSH
443 / TCP	Tiebreaker	MetroCluster management LIFs	Secure communications via HTTP (SSL)
22 / TCP	Tiebreaker	MetroCluster management LIFs	Secure communications via SSH
162 / UDP	Tiebreaker	SNMP trap host	Used to send alert notification SNMP traps
ICMP (ping)	Tiebreaker	MetroCluster management LIFs	Check if cluster IP is reachable
ICMP (ping)	Tiebreaker	MetroCluster management LIFs	Check if node IP is reachable

Where to find additional information

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

MetroCluster and miscellaneous guides

Guide	Content
ONTAP 9 Documentation Center	• All MetroCluster guides
NetApp Technical Report 4375: NetApp MetroCluster for ONTAP 9.3	• A technical overview of the MetroCluster configuration and operation. • Best practices for MetroCluster 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

Guide	Content
Stretch MetroCluster installation and configuration	• Stretch MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • Configuring the MetroCluster in ONTAP
MetroCluster IP installation and configuration	• MetroCluster IP architecture • Cabling the MetroCluster IP configuration • Configuring the MetroCluster in ONTAP
MetroCluster Maintenance Guide	• Guidelines for maintenance in a MetroCluster configuration • Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches • Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster configuration • Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster configuration • Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster configuration • Expanding a two-node fabric-attached or stretch MetroCluster configuration to a four-node MetroCluster configuration. • Expanding a four-node fabric-attached or stretch MetroCluster configuration to an eight-node MetroCluster configuration.
Active IQ Unified Manager documentation NetApp Documentation: Product Guides and Resources	• Monitoring the MetroCluster configuration and performance
Copy-based transition	• Transitioning data from 7-Mode storage systems to clustered storage systems

Understand MetroCluster data protection and disaster recovery

Understanding MetroCluster data protection and disaster recovery

It is helpful to understand how MetroCluster protects data and provides transparent recovery from failures so that you can manage your switchover and switchback activities easily and efficiently.

MetroCluster uses mirroring to protect the data in a cluster. It provides disaster recovery through a single MetroCluster command that activates a secondary on the survivor site to serve the mirrored data originally owned by a primary site affected by disaster.

How eight- and four-node MetroCluster configurations provide local failover and switchover

Eight- and four-node MetroCluster configurations protect data on both a local level and cluster level. If you are setting up a MetroCluster configuration, you need to know how MetroCluster configurations protect your data.

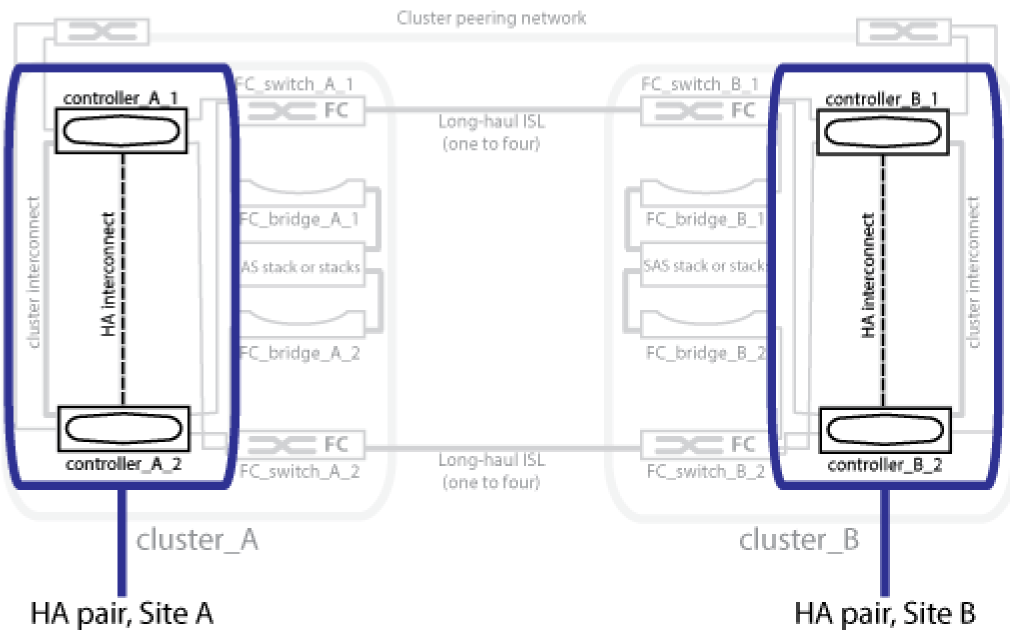
MetroCluster configurations protect data by using two physically separated, mirrored clusters. Each cluster synchronously mirrors the data and storage virtual machine (SVM) configuration of the other. When a disaster occurs at one site, an administrator can activate the mirrored SVM and begin serving the mirrored data from the surviving site. Additionally, the nodes in each cluster are configured as an HA pair, providing a level of local failover.

How local HA data protection works in a MetroCluster configuration

You need to understand how HA pairs work in the MetroCluster configuration.

The two clusters in the peered network provide bidirectional disaster recovery, where each cluster can be the source and backup of the other cluster. Each cluster includes two nodes, which are configured as an HA pair. In the case of a failure or required maintenance within a single node’s configuration, storage failover can transfer that node’s operations to its local HA partner.

The following illustration shows a MetroCluster FC configuration. The HA functionality is the same in MetroCluster IP configurations, except that the HA interconnect is provided by the cluster switches.



Related information

High-availability configuration

How MetroCluster configurations provide data and configuration replication

MetroCluster configurations use a variety of ONTAP features to provide synchronous replication of data and configuration between the two MetroCluster sites.

Configuration protection with the configuration replication service

The ONTAP configuration replication service (CRS) protects the MetroCluster configuration by automatically replicating the information to the DR partner.

The CRS synchronously replicates local node configuration to the DR partner in the partner cluster. This replication is carried out over the cluster peering network.

The information replicated includes the cluster configuration and the SVM configuration.

Replication of SVMs during MetroCluster operations

The ONTAP configuration replication service (CRS) provides redundant data server configuration and mirroring of data volumes that belong to the SVM. If a switchover occurs, the source SVM is brought down and the destination SVM, located on the surviving cluster, becomes active.

> ⓘ Destination SVMs in the MetroCluster configuration have the suffix “-mc” automatically appended to their name to help identify them. A MetroCluster configuration appends the suffix “-mc” to the name of the destination SVMs, if the SVM name contains a period, the suffix “-mc” is applied prior to the first period. For example, if the SVM name is SVM.DNS.NAME, then the suffix “-mc” is appended as SVM-MC.DNS.NAME.

The following example shows the SVMs for a MetroCluster configuration, where SVM_cluster_A is an SVM on the source site and SVM_cluster_A-mc is a sync-destination aggregate on the disaster recovery site.

- SVM_cluster_A serves data on cluster A.

  It is a sync-source SVM that represents the SVM configuration (LIFs, protocols, and services) and data in volumes belonging to the SVM. The configuration and data are replicated to SVM_cluster_A-mc, a sync-destination SVM located on cluster B.

- SVM_cluster_B serves data on cluster B.

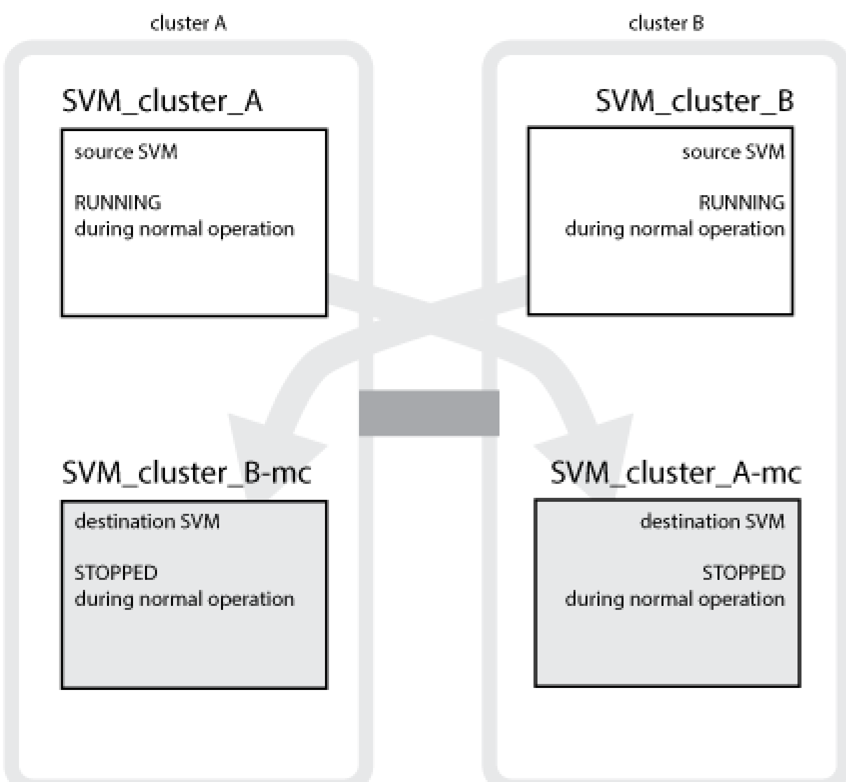
  It is a sync-source SVM that represents configuration and data to SVM_cluster_B-mc located on cluster A.

- SVM_cluster_B-mc is a sync-destination SVM that is stopped during normal, healthy operation of the MetroCluster configuration.

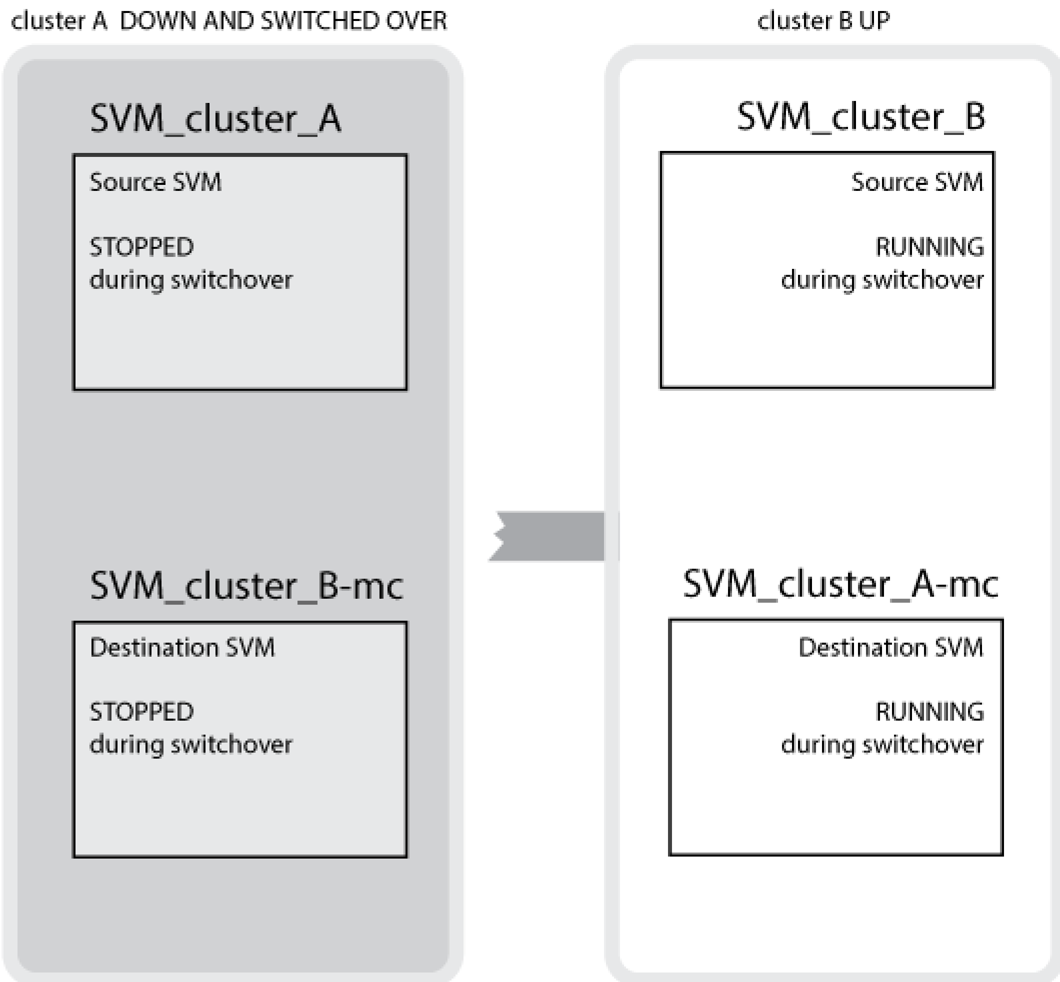
  In a successful switchover from cluster B to cluster A, SVM_cluster_B is stopped and SVM_cluster_B-mc is activated and begins serving data from cluster A.

- SVM_cluster_A-mc is a sync-destination SVM that is stopped during normal, healthy operation of the MetroCluster configuration.

  In a successful switchover from cluster A to cluster B, SVM_cluster_A is stopped and SVM_cluster_A-mc is activated and begins serving data from cluster B.



If a switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving the data.



The availability of remote plexes after switchover depends on the MetroCluster configuration type:

- For MetroCluster FC configurations, after switchover, both local and remote plexes remain online if the disaster site storage is accessible via the ISLs.

  If the ISLs have failed and the disaster site storage is not available, the sync-destination SVM begins serving data from the surviving site.

- For MetroCluster IP configurations the availability of the remote plexes depends on the ONTAP version:
  - Starting with ONTAP 9.5, both local and remote plexes remain online if the disaster site nodes remain booted up.
  - Prior to ONTAP 9.5, storage is available only from local plex on the surviving site.

    The sync-destination SVM begins serving data from the surviving site.

Related information

System administration

How MetroCluster configurations use SyncMirror to provide data redundancy

Mirrored aggregates using SyncMirror functionality provide data redundancy and contain the volumes owned by the source and destination storage virtual machine (SVM). Data is replicated into disk pools on the partner cluster. Unmirrored aggregates are also supported.

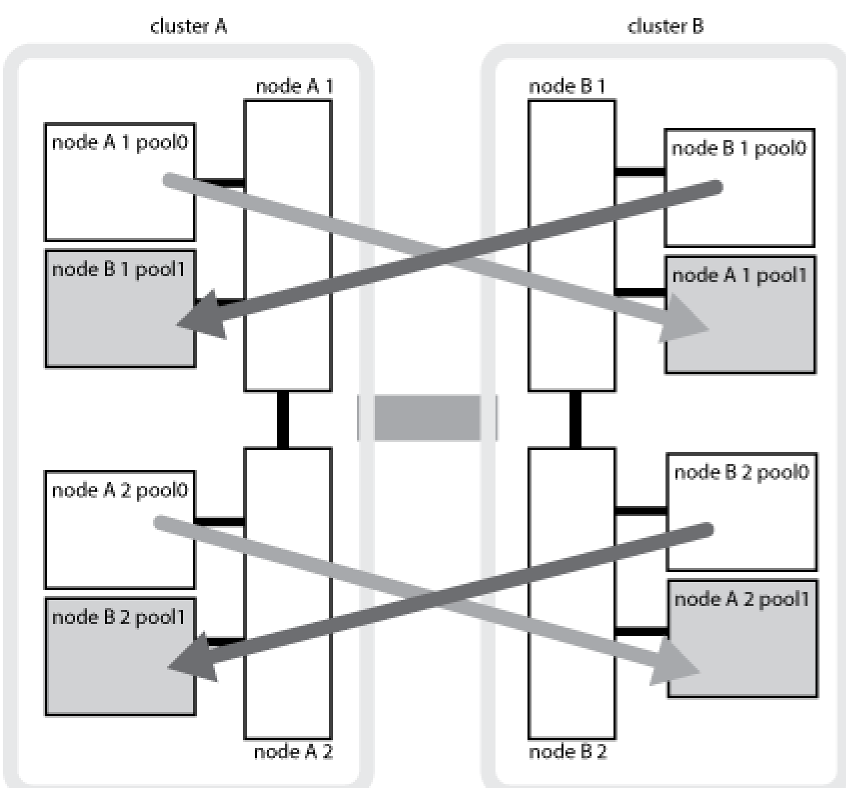
The following table shows the state (online or offline) of an unmirrored aggregate after a switchover:

Type of switchover	State
Negotiated switchover (NSO)	Online
Automatic unplanned switchover (AUSO)	Online
Unplanned switchover (USO)	• If storage is not available: Offline • If storage is available: Online

NOTE: After a switchover, if the unmirrored aggregate is at the DR partner node and there is an inter-switch link (ISL) failure, then that local node might fail.

The following illustration shows how disk pools are mirrored between the partner clusters. Data in local plexes (in pool0) is replicated to remote plexes (in pool1).

> ⓘ If hybrid aggregates are used, performance degradation can occur after a SyncMirror plex has failed due to the solid-state disk (SSD) layer filling up.



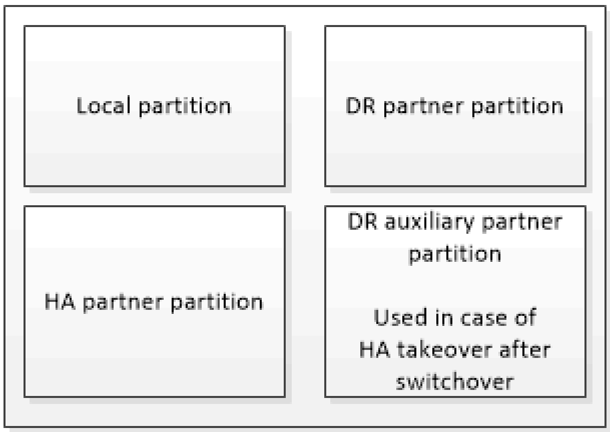
How NVRAM or NVMEM cache mirroring and dynamic mirroring work in MetroCluster configurations

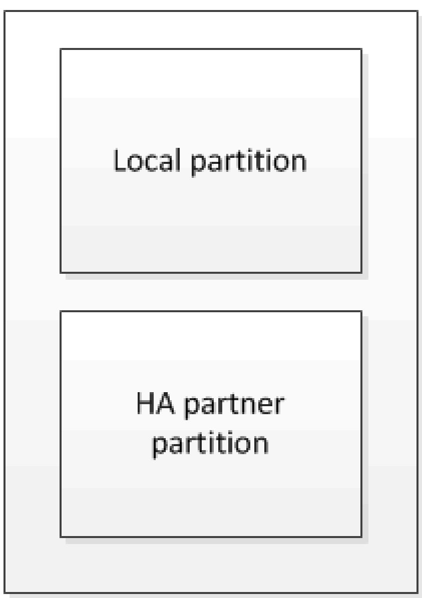
The nonvolatile memory (NVRAM or NVMEM, depending on the platform model) in the storage controllers is mirrored both locally to a local HA partner and remotely to a remote disaster recovery (DR) partner on the partner site. In the event of a local failover or switchover, this configuration enables data in the nonvolatile cache to be preserved.

In an HA pair that is not part of a MetroCluster configuration, each storage controller maintains two nonvolatile cache partitions: one for itself and one for its HA partner.

In a four-node MetroCluster configuration, the nonvolatile cache of each storage controller is divided into four partitions. In a two-node MetroCluster configuration, the HA partner partition and DR auxiliary partition are not used, because the storage controllers are not configured as an HA pair.

Nonvolatile caches for a storage controller
In a MetroCluster configuration
In a non-MetroCluster HA pair





The nonvolatile caches store the following content:

- The local partition holds data that the storage controller has not yet written to disk.
- The HA partner partition holds a copy of the local cache of the storage controller’s HA partner.

In a two-node MetroCluster configuration, there is no HA partner partition because the storage controllers are not configured as an HA pair.

- The DR partner partition holds a copy of the local cache of the storage controller's DR partner.

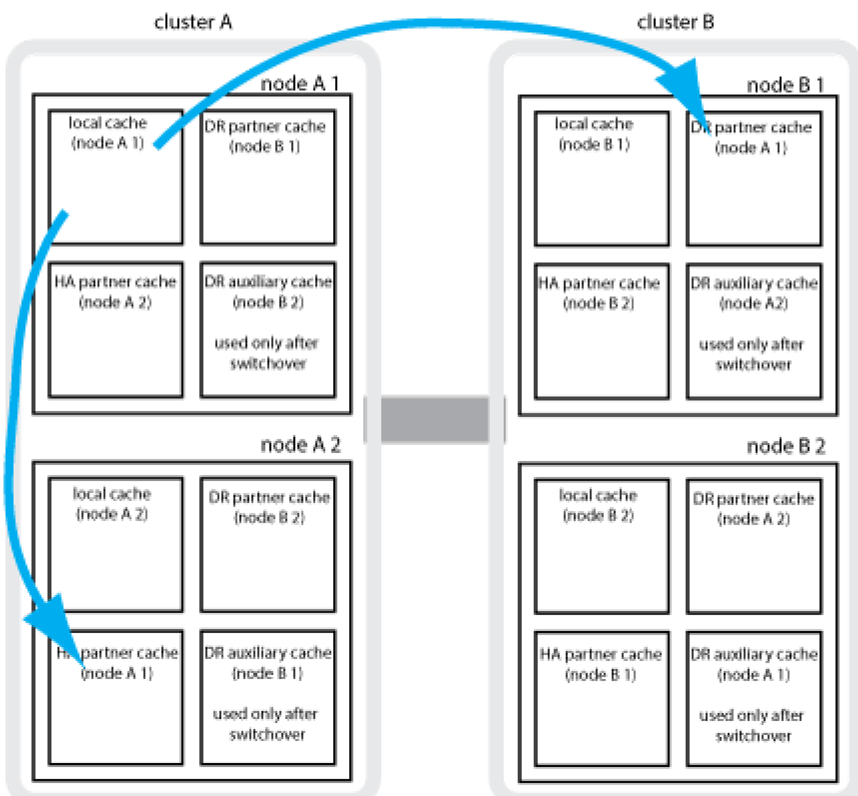
  The DR partner is a node in the partner cluster that is paired with the local node.

- The DR auxiliary partner partition holds a copy of the local cache of the storage controller's DR auxiliary partner.

  The DR auxiliary partner is the HA partner of the local node's DR partner. This cache is needed if there is an HA takeover (either when the configuration is in normal operation or after a MetroCluster switchover).

  In a two-node MetroCluster configuration, there is no DR auxiliary partner partition because the storage controllers are not configured as an HA pair.

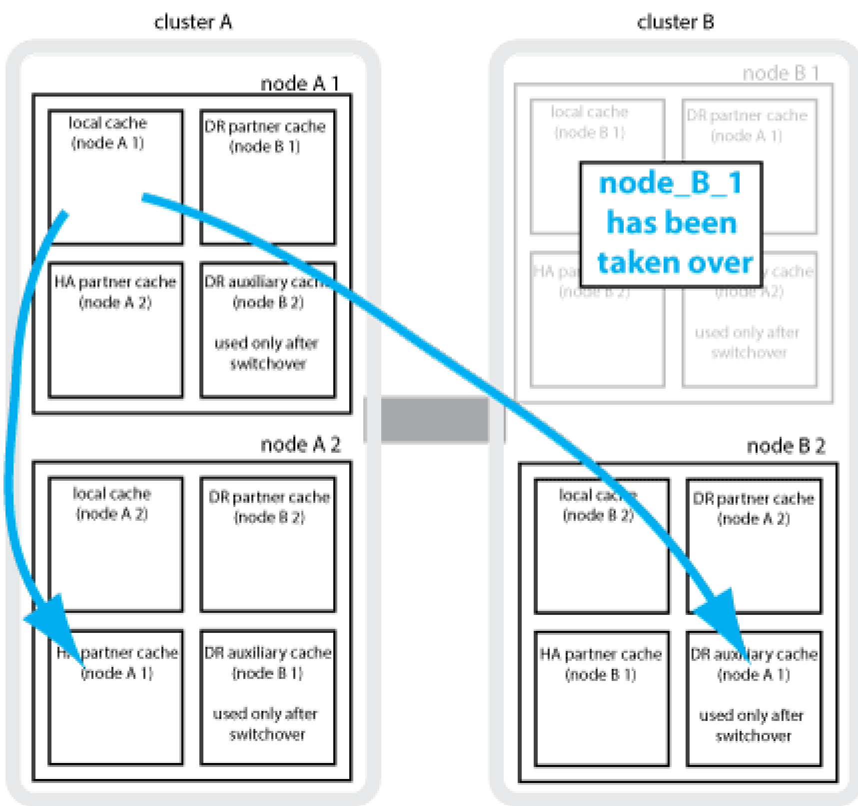
For example, the local cache of a node (node_A_1) is mirrored both locally and remotely at the MetroCluster sites. The following illustration shows that the local cache of node_A_1 is mirrored to the HA partner (node_A_2) and DR partner (node_B_1):



Dynamic mirroring in event of a local HA takeover

If a local HA takeover occurs in a four-node MetroCluster configuration, the taken-over node can no longer act as a mirror for its DR partner. To allow DR mirroring to continue, the mirroring automatically switches to the DR auxiliary partner. After a successful giveback, mirroring automatically returns to the DR partner.

For example, node_B_1 fails and is taken over by node_B_2. The local cache of node_A_1 can no longer be mirrored to node_B_1. The mirroring switches to the DR auxiliary partner, node_B_2.



Types of disasters and recovery methods

You need to be familiar with different types of failures and disasters so that you can use the MetroCluster configuration to respond appropriately.

- Single-node failure

  A single component in the local HA pair fails.

  In a four-node MetroCluster configuration, this failure might lead to an automatic or a negotiated takeover of the impaired node, depending on the component that failed. Data recovery is described in the *High Availability Configuration Guide*.

  In a two-node MetroCluster configuration, this failure leads to an automatic unplanned switchover (AUSO).

- Site-wide controller failure

  All controller modules fail at a site because of loss of power, replacement of equipment, or disaster. Typically, MetroCluster configurations cannot differentiate between failures and disasters. However, witness software, such as the MetroCluster Tiebreaker software, can differentiate between them. A site-wide controller failure condition can lead to an automatic switchover if Inter-Switch Link (ISL) links and switches are up and the storage is accessible.

  The *High-Availability Configuration Guide* has more information about how to recover from site-wide controller failures that do not include controller failures, as well as failures that include of one or more controllers.

- ISL failure

  The links between the sites fail. The MetroCluster configuration takes no action. Each node continues to serve data normally, but the mirrors are not written to the respective disaster recovery sites because access to them is lost.

- Multiple sequential failures

  Multiple components fail in a sequence. For example, a controller module, a switch fabric, and a shelf fail in a sequence and result in a storage failover, fabric redundancy, and SyncMirror sequentially protecting against downtime and data loss.

The following table shows failure types, and the corresponding disaster recovery (DR) mechanism and recovery method:

AUSO (automatic unscheduled switchover) is not supported on MetroCluster IP configurations.

Failure type	DR mechanism		Summary of recovery method	
	Four-node configuration	**Two-node configuration**	**Four-node configuration**	**Two-node configuration**
Single-node failure	Local HA failover	AUSO	Not required if automatic failover and giveback is enabled.	After the node is restored, manual healing and switchback using the metrocluster heal -phase aggregates, metrocluster heal -phase root-aggregates, and metrocluster switchback commands is required. NOTE: The metrocluster heal commands are not required on MetroCluster IP configurations running ONTAP 9.5 or later.

<table>
<tr><th>Failure type</th><th colspan="2">DR mechanism</th><th>Summary of recovery method</th></tr>
<tr><td>Site failure</td><td colspan="2">MetroCluster switchover</td><td rowspan="3">After the node is restored, manual healing and switchback using the metrocluster healing and metrocluster switchback commands is required.

The metrocluster heal commands are not required on MetroCluster IP configurations running ONTAP 9.5.</td></tr>
<tr><td>Site-wide controller failure</td><td>AUSO Only if the storage at the disaster site is accessible.</td><td>AUSO (same as single-node failure)</td></tr>
<tr><td>Multiple sequential failures</td><td>Local HA failover followed by MetroCluster forced switchover using the metrocluster switchover -forced -on-disaster command.

NOTE: Depending on the component that failed, a forced switchover might not be required.</td><td>MetroCluster forced switchover using the metrocluster switchover -forced -on-disaster command.</td></tr>
<tr><td>ISL failure</td><td colspan="2">No MetroCluster switchover; the two clusters independently serve their data</td><td>Not required for this type of failure. After you restore connectivity, the storage resynchronizes automatically.</td></tr>
</table>

How an eight-node or four-node MetroCluster configuration provides nondisruptive operations

In the case of an issue limited to a single node, a failover and giveback within the local HA pair provides continued nondisruptive operation. In this case, the MetroCluster configuration does not require a switchover to the remote site.

Because the eight-node or four-node MetroCluster configuration consists of one or more HA pair at each site, each site can withstand local failures and perform nondisruptive operations without requiring a switchover to the partner site. The operation of the HA pair is the same as HA pairs in non-MetroCluster configurations.

For four-node and eight-node MetroCluster configurations, node failures due to panic or power loss can cause an automatic switchover.

High-availability configuration

If a second failure occurs after a local failover, the MetroCluster switchover event provides continued nondisruptive operations. Similarly, after a switchover operation, in the event of a second failure in one of the surviving nodes, a local failover event provides continued nondisruptive operations. In this case, the single surviving node serves data for the other three nodes in the DR group.

Switchover and switchback during MetroCluster transition

MetroCluster FC-to-IP transition involves adding MetroCluster IP nodes and IP switches to an existing MetroCluster FC configuration, and then retiring the MetroCluster FC nodes. Depending on the stage of the transition process, the MetroCluster switchover, healing, and switchback operations use different workflows.

See Switchover, healing, and switchback operations during transition.

Consequences of local failover after switchover

If a MetroCluster switchover occurs, and then an issue arises at the surviving site, a local failover can provide continued, nondisruptive operation. However, the system is at risk because it is no longer in a redundant configuration.

If a local failover occurs after a switchover has occurred, a single controller serves data for all storage systems in the MetroCluster configuration, leading to possible resource issues, and is vulnerable to additional failures.

How a two-node MetroCluster configuration provides nondisruptive operations

If one of the two sites has an issue due to panic, the MetroCluster switchover provides continued nondisruptive operation. If the power loss impacts both the node and the storage, then the switchover is not automatic and there is a disruption until the metrocluster switchover command is issued.

Because all storage is mirrored, a switchover operation can be used to provide nondisruptive resiliency in case of a site failure similar to that found in a storage failover in an HA pair for a node failure.

For two-node configurations, the same events that trigger an automatic storage failover in an HA pair trigger an automatic unplanned switchover (AUSO). This means that a two-node MetroCluster configuration has the same level of protection as an HA pair.

Related information

Automatic unplanned switchover in MetroCluster FC configurations

Overview of the switchover process

The MetroCluster switchover operation enables immediate resumption of services following a disaster by moving storage and client access from the source cluster to the remote site. You must be aware of what changes to expect and which actions you need to perform if a switchover occurs.

During a switchover operation, the system takes the following actions:

- Ownership of the disks that belong to the disaster site is changed to the disaster recovery (DR) partner.

  This is similar to the case of a local failover in a high-availability (HA) pair, in which ownership of the disks belonging to the partner that is down is changed to the healthy partner.

- The surviving plexes that are located on the surviving site but belong to the nodes in the disaster cluster are brought online on the cluster at the surviving site.
- The sync-source storage virtual machine (SVM) that belongs to the disaster site is brought down only during a negotiated switchover.

  > ⓘ This is applicable only to a negotiated switchover.

- The sync-destination SVM belonging to the disaster site is brought up.

While being switched over, the root aggregates of the DR partner are not brought online.

The metrocluster switchover command switches over the nodes in all DR groups in the MetroCluster configuration. For example, in an eight-node MetroCluster configuration, it switches over the nodes in both DR groups.

If you are switching over only services to the remote site, you should perform a negotiated switchover without fencing the site. If storage or equipment is unreliable, you should fence the disaster site, and then perform an unplanned switchover. Fencing prevents RAID reconstructions when the disks power up in a staggered manner.

> ⓘ This procedure should be only used if the other site is stable and not intended to be taken offline.

Availability of commands during switchover

The following table shows the availability of commands during switchover:

Command	Availability
`storage aggregate create`	You can create an aggregate: • If it is owned by a node that is part of the surviving cluster You cannot create an aggregate: • For a node at the disaster site • For a node that is part of the surviving cluster
`storage aggregate delete`	You can delete a data aggregate.
`storage aggregate mirror`	You can create a plex for a non-mirrored aggregate.
`storage aggregate plex delete`	You can delete a plex for a mirrored aggregate.
`vserver create`	You can create an SVM: • If its root volume resides in a data aggregate owned by the surviving cluster You cannot create an SVM: • If its root volume resides in a data aggregate owned by the disaster-site cluster
`vserver delete`	You can delete both sync-source and sync-destination SVMs.

Command	Availability
`network interface create -lif`	You can create a data SVM LIF for both sync-source and sync-destination SVMs.
`network interface delete -lif`	You can delete a data SVM LIF for both sync-source and sync-destination SVMs.
`volume create`	You can create a volume for both sync-source and sync-destination SVMs. • For a sync-source SVM, the volume must reside in a data aggregate owned by the surviving cluster • For a sync-destination SVM, the volume must reside in a data aggregate owned by the disaster-site cluster
`volume delete`	You can delete a volume for both sync-source and sync-destination SVMs.
`volume move`	You can move a volume for both sync-source and sync-destination SVMs. • For a sync-source SVM, the surviving cluster must own the destination aggregate • For a sync-destination SVM, the disaster-site cluster must own the destination aggregate
`snapmirror break`	You can break a SnapMirror relationship between a source and destination endpoint of a data protection mirror.

Differences in switchover between MetroCluster FC and IP configurations

In MetroCluster IP configurations, because the remote disks are accessed through the remote DR partner nodes acting as iSCSI targets, the remote disks are not accessible when the remote nodes are taken down in a switchover operation. This results in differences with MetroCluster FC configurations:

- Mirrored aggregates that are owned by the local cluster become degraded.
- Mirrored aggregates that were switched over from the remote cluster become degraded.

> When unmirrored aggregates are supported on a MetroCluster IP configuration, the unmirrored aggregates that are not switched over from the remote cluster are not accessible.

Disk ownership changes during HA takeover and MetroCluster switchover in a four-node MetroCluster configuration

The ownership of disks temporarily changes automatically during high availability and

MetroCluster operations. It is helpful to know how the system tracks which node owns which disks.

In ONTAP, a controller module’s unique system ID (obtained from a node’s NVRAM card or NVMEM board) is used to identify which node owns a specific disk. Depending on the HA or DR state of the system, the ownership of the disk might temporarily change. If the ownership changes because of an HA takeover or a DR switchover, the system records which node is the original (called “home”) owner of the disk, so that it can return the ownership after HA giveback or DR switchback. The system uses the following fields to track disk ownership:

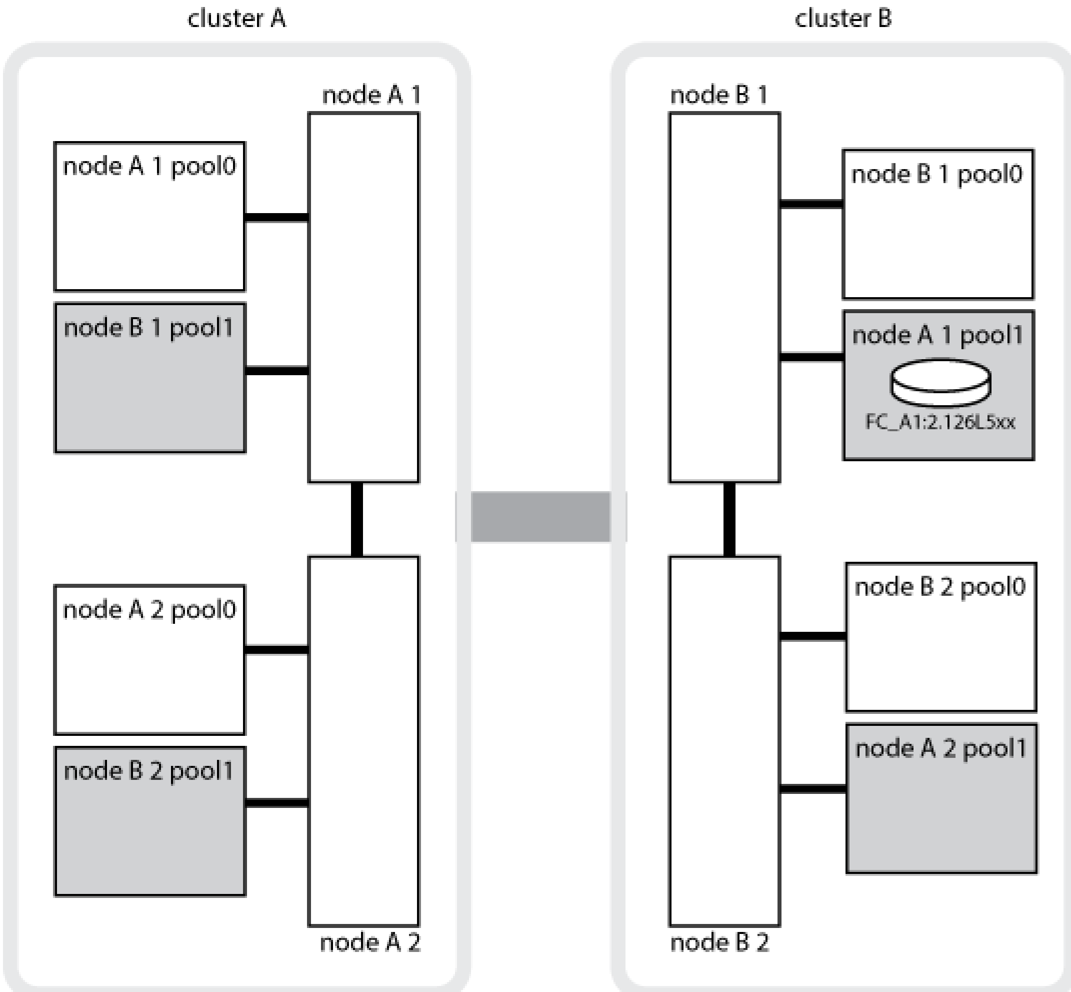
- Owner
- Home owner
- DR Home owner

In the MetroCluster configuration, in the event of a switchover, a node can take ownership of an aggregate originally owned by nodes in the partner cluster. Such aggregates are referred to as cluster-foreign aggregates. The distinguishing feature of a cluster-foreign aggregate is that it is an aggregate not currently known to the cluster, and so the DR Home owner field is used to show that it is owned by a node from the partner cluster. A traditional foreign aggregate within an HA pair is identified by Owner and Home owner values being different, but the Owner and Home owner values are the same for a cluster-foreign aggregate; thus, you can identify a cluster-foreign aggregate by the DR Home owner value.

As the state of the system changes, the values of the fields change, as shown in the following table:

	Value during…
Field	Normal operation
Local HA takeover	MetroCluster switchover
Takeover during switchover	Owner
ID of the node that has access to the disk.	ID of the HA partner, which temporarily has access to the disk.
ID of the DR partner, which temporarily has access to the disk.	ID of the DR auxiliary partner, which temporarily has access to the disk.
Home owner	ID of the original owner of the disk within the HA pair.
ID of the original owner of the disk within the HA pair.	ID of the DR partner, which is the Home owner in the HA pair during the switchover.
ID of the DR partner, which is the Home owner in the HA pair during the switchover.	DR Home owner
Empty	Empty
ID of the original owner of the disk within the MetroCluster configuration.	ID of the original owner of the disk within the MetroCluster configuration.

The following illustration and table provide an example of how ownership changes, for a disk in node_A_1's disk pool1, physically located in cluster_B.



MetroCluster state	Owner	Home owner	DR Home owner	Notes
Normal with all nodes fully operational.	node_A_1	node_A_1	not applicable	
Local HA takeover, node_A_2 has taken over disks belonging to its HA partner node_A_1.	node_A_2	node_A_1	not applicable	

MetroCluster state	Owner	Home owner	DR Home owner	Notes
DR switchover, node_B_1 has taken over disks belong to its DR partner, node_A_1.	node_B_1	node_B_1	node_A_1	The original home node ID is moved to the DR Home owner field. After aggregate switchback or healing, ownership goes back to node_A_1.
In DR switchover and local HA takeover (double failure), node_B_2 has taken over disks belonging to its HA node_B_1.	node_B_2	node_B_1	node_A_1	After giveback, ownership goes back to node_B_1. After switchback or healing, ownership goes back to node_A_1.
After HA giveback and DR switchback, all nodes fully operational.	node_A_1	node_A_1	not applicable	

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 are 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 metadata volume and data SVM root volumes

The configuration replication service (CRS) metadata volume and data SVM 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

SVMs 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.

Considerations for unmirrored aggregates and SAN

A LUN should not be located on an unmirrored aggregate. Configuring a LUN on an unmirrored aggregate can result in a switchover operation that exceeds 120 seconds and a data outage.

Automatic unplanned switchover in MetroCluster FC configurations

In MetroCluster FC configurations, certain scenarios can trigger an automatic unplanned switchover (AUSO) in the event of a site-wide controller failure to provide nondisruptive operations. AUSO can be disabled if desired.

> Automatic unplanned switchover is not supported in MetroCluster IP configurations.

In a MetroCluster FC configuration, an AUSO can be triggered if all nodes at a site are failed because of the following reasons:

- Power down
- Power loss
- Power panic

> In an eight-node MetroCluster FC configuration, you can set an option to trigger an AUSO if both nodes in an HA pair fail.

Because there is no local HA failover available in a two-node MetroCluster configuration, the system performs an AUSO to provide continued operation after a controller failure. This functionality is similar to the HA takeover capability in an HA pair. In a two-node MetroCluster configuration, an AUSO can be triggered in the following scenarios:

- Node power down
- Node power loss
- Node panic
- Node reboot

If an AUSO occurs, disk ownership for the impaired node's pool0 and pool1 disks is changed to the disaster recovery (DR) partner. This ownership change prevents the aggregates from going into a degraded state after the switchover.

After the automatic switchover, you must manually proceed through the healing and switchback operations to return the controller to normal operation.

Hardware-assisted AUSO in two-node MetroCluster configurations

In a two-node MetroCluster configuration, the controller module's service processor (SP) monitors the configuration. In some scenarios, the SP can detect a failure faster than the ONTAP software. In this case, the SP triggers AUSO. This feature is automatically enabled.

The SP sends and receives SNMP traffic to and from its DR partner to monitor its health.

Changing the AUSO setting in MetroCluster FC configurations

AUSO is set to auso-on-cluster-disaster by default. Its status can be viewed in the metrocluster show command.

> ⓘ The AUSO setting does not apply to MetroCluster IP configurations.

You can disable AUSO with the 'metrocluster modify -auto-switchover-failure-domain auto-disabled' command. This command prevents triggering AUSO in DR site-wide controller failure. It should be run on both the sites if you want to disable AUSO on both the sites.

AUSO can be reenabled with the metrocluster modify -auto-switchover-failure-domain auso-on-cluster-disaster command.

AUSO can also be set to auso-on-dr-group-disaster. This advance level command triggers AUSO on HA failover at one site. It should be run on both the sites with the metrocluster modify -auto-switchover-failure -domain auso-on-dr-group-disaster command.

The AUSO setting during switchover

When switchover occurs, the AUSO setting is disabled internally because if a site is in switchover, it cannot automatically switch over.

Recovering from AUSO

To recover from an AUSO, you perform the same steps as for a planned switchover.

Performing switchover for tests or maintenance

Mediator-assisted automatic unplanned switchover in MetroCluster IP configurations

In MetroCluster IP configurations, the system can use the ONTAP Mediator to detect failures and perform a Mediator-assisted automatic unplanned switchover (MAUSO).

> ⓘ MAUSO is not supported in MetroCluster FC configurations.

The ONTAP Mediator provides mailbox LUNs for the MetroCluster IP nodes. These LUNs are colocated with the ONTAP Mediator, which runs on a Linux host physically separate from the MetroCluster sites.

The MetroCluster nodes use the mailbox information to determine if a MAUSO is required. MAUSO will not be initiated if the nonvolatile memory (NVRAM or NVMEM, depending on the platform model) in the storage controllers is not mirrored to the remote disaster recovery (DR) partner on the partner site

What happens during healing (MetroCluster FC configurations)

During healing in MetroCluster FC configurations, the resynchronization of mirrored aggregates occurs in a phased process that prepares the nodes at the repaired disaster site for switchback. It is a planned event, thereby giving you full control of each step to minimize downtime. Healing is a two-step process that occurs on the storage and controller components.

Data aggregate healing

After the problem at the disaster site is resolved, you start the storage healing phase:

1. Checks that all nodes are up and running at the surviving site.
2. Changes ownership of all the pool 0 disks at the disaster site, including root aggregates.

During this phase of healing, the RAID subsystem resynchronizes mirrored aggregates, and the WAFL subsystem replays the nvsave files of mirrored aggregates that had a failed pool 1 plex at the time of switchover.

If some source storage components failed, the command reports the errors at applicable levels: Storage, Sanown, or RAID.

If no errors are reported, the aggregates are successfully resynchronized. This process can sometimes take hours to complete.

Healing the configuration

Root aggregate healing

After the aggregates are synchronized, you start the controller healing phase by giving back the CFO aggregates and root aggregates to their respective DR partners.

Healing the configuration

What happens during healing (MetroCluster IP configurations)

During healing in MetroCluster IP configurations, the resynchronization of mirrored aggregates occurs in a phased process that prepares the nodes at the repaired disaster site for switchback. It is a planned event, thereby giving you full control of each step to minimize downtime. Healing is a two-step process that occurs on the storage and controller components.

Differences with MetroCluster FC configurations

In MetroCluster IP configurations, you must boot the nodes in the disaster site cluster before the healing operation is performed.

The nodes in the disaster site cluster must be running so that the remote iSCSI disks can be accessed when aggregates are resynchronized.

If the disaster site nodes are not running, the healing operation fails because the disaster node cannot perform the disk ownership changes needed.

Data aggregate healing

After the problem at the disaster site is resolved, you start the storage healing phase:

1. Checks that all nodes are up and running at the surviving site.
2. Changes ownership of all the pool 0 disks at the disaster site, including root aggregates.

During this phase of healing, the RAID subsystem resynchronizes mirrored aggregates, and the WAFL subsystem replays the nvsave files of mirrored aggregates that had a failed pool 1 plex at the time of switchover.

If some source storage components failed, the command reports the errors at applicable levels: Storage, Sanown, or RAID.

If no errors are reported, the aggregates are successfully resynchronized. This process can sometimes take hours to complete.

Healing the configuration

Root aggregate healing

After the aggregates are synchronized, you perform the root aggregate healing phase. In MetroCluster IP configurations, this phase confirms that aggregates have been healed.

Healing the configuration

Automatic healing of aggregates on MetroCluster IP configurations after switchover

Starting with ONTAP 9.5, healing is automated during negotiated switchover operations on MetroCluster IP configurations. Starting with ONTAP 9.6, automated healing after unscheduled switchover is supported. This removes the requirement to issue the metrocluster heal commands.

Automatic healing after negotiated switchover (starting with ONTAP 9.5)

After performing a negotiated switchover (a switchover command issued without the -forced-on-disaster true option), the automatic healing functionality simplifies the steps required to return the system to normal operation. On systems with automatic healing, the following occurs after the switchover:

- The disaster site nodes remain up.

  Because they are in switchover state, they are not serving data from their local mirrored plexes.

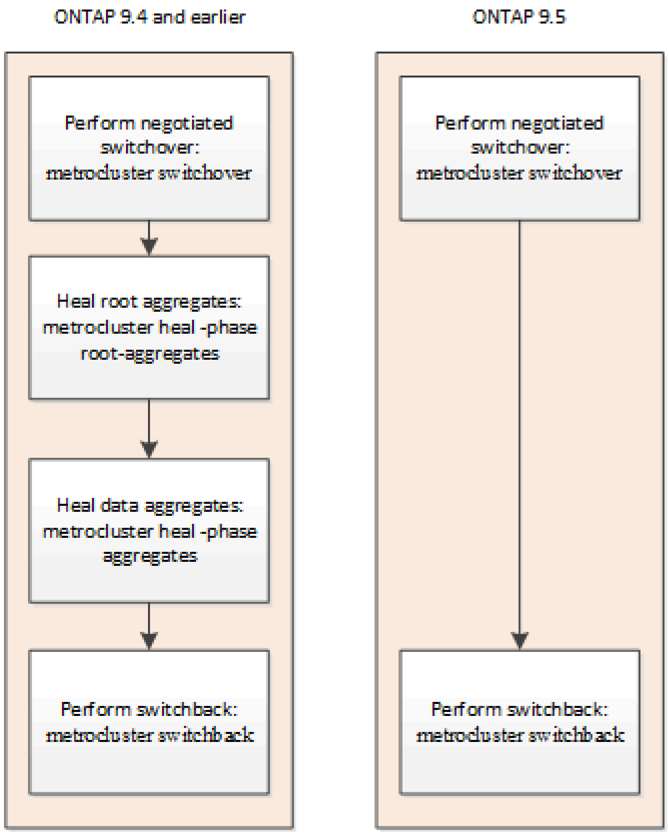
- The disaster site nodes are moved to the `Waiting for switchback` state.

  You can confirm the status of the disaster site nodes by using the metrocluster operation show command.

- You can perform the switchback operation without issuing the healing commands.

This feature applies to MetroCluster IP configurations running ONTAP 9.5 and later. It does not apply to MetroCluster FC configurations.

The manual healing commands are still required on MetroCluster IP configurations running ONTAP 9.4 and earlier.



Automatic healing after unscheduled switchover (starting with ONTAP 9.6)

Automatic healing after an unscheduled switchover is supported on MetroCluster IP configurations starting with ONTAP 9.6. An unscheduled switchover is one in which in you issue the switchover command with the -forced -on-disaster true option.

Automatic healing after an unscheduled switchover is not supported on MetroCluster FC configurations, and the manual healing commands are still required after unscheduled switchover on MetroCluster IP configurations running ONTAP 9.5 and earlier.

On systems running ONTAP 9.6 and later, the following occurs after the unscheduled switchover:

- Depending on the extent of the disaster, the disaster site nodes can be down.

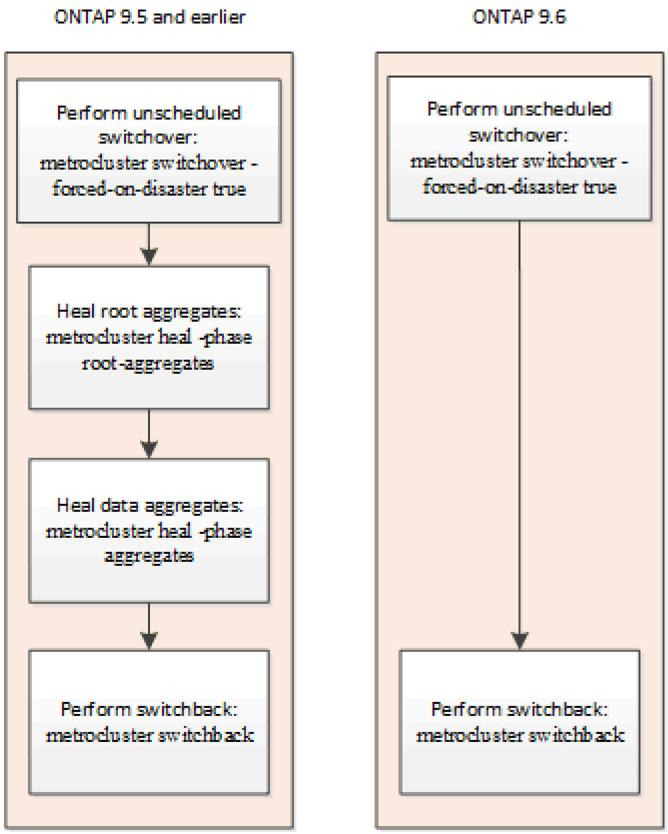
  Because they are in switchover state, they are not serving data from their local mirrored plexes, even if they are powered up.

- If the disaster sites were down, when booted up, the disaster site nodes are moved to the `Waiting for switchback` state.

  If the disaster sites remained up, they are immediately moved to the `Waiting for switchback` state.

- The healing operations are performed automatically.

  You can confirm the status of the disaster site nodes, and that healing operations succeeded, by using the metrocluster operation show command.



If automatic healing fails

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 9.6. You can use the metrocluster operation show and metrocluster operation history show -instance commands to monitor the status of healing and determine the cause of a failure.

Creating SVMs for a MetroCluster configuration

You can create SVMs for a MetroCluster configuration to provide synchronous disaster recovery and high availability of data on clusters that are set up for a MetroCluster configuration.

- The two clusters must be in a MetroCluster configuration.
- Aggregates must be available and online in both clusters.
- If required, IPspaces with the same names must be created on both clusters.
- If one of the clusters forming the MetroCluster configuration is rebooted without utilizing a switchover, then the sync-source SVMs might come online as `stopped` rather than `started`.

When you create an SVM on one of the clusters in a MetroCluster configuration, the SVM is created as the source SVM, and the partner SVM is automatically created with the same name but with the “-mc” suffix on the partner cluster. If the SVM name contains a period, the “-mc” suffix is applied prior to the first period, for example, SVM-MC.DNS.NAME.

In a MetroCluster configuration, you can create 64 SVMs on a cluster. A MetroCluster configuration supports 128 SVMs.

1. Use the vserver create command.

   The following example shows the SVM with the subtype sync-source on the local site and the SVM with the subtype sync-destination on the partner site:

   ```
   cluster_A::>vserver create -vserver vs4 -rootvolume vs4_root -aggregate
   aggr1
   -rootvolume-security-style mixed
   [Job 196] Job succeeded:
   Vserver creation completed
   ```

   The SVM vs4 is created on the local site and the SVM vs4-mc is created on the partner site.

2. View the newly created SVMs.

   ◦ On the local cluster, verify the configuration state of SVMs: `metrocluster vserver show`

     The following example shows the partner SVMs and their configuration state:

     ```
     cluster_A::> metrocluster vserver show

                           Partner    Configuration
     Cluster     Vserver   Vserver    State
     ---------  --------  --------- -----------------
     cluster_A   vs4       vs4-mc     healthy
     cluster_B   vs1       vs1-mc     healthy
     ```

   ◦ From the local and partner clusters, verify the state of the newly configured SVMs: `vserver show command`

     The following example displays the administrative and operational states of the SVMs:

```
cluster_A::> vserver show

                              Admin   Operational Root
Vserver Type  Subtype         State   State       Volume     Aggregate
------- ----- -------       ------- --------    -----------
----------
vs4     data  sync-source   running   running    vs4_root   aggr1

cluster_B::> vserver show

                                Admin   Operational  Root
Vserver Type  Subtype           State   State        Volume
Aggregate
------- ----- -------           ------  ---------    -----------
----------
vs4-mc  data  sync-destination running stopped      vs4_root    aggr1
```

SVM creation might fail if any intermediate operations, such as root volume creation, fail and the SVM is in the `initializing` state. You must delete the SVM and re-create it.

The SVMs for the MetroCluster configuration are created with a root volume size of 1 GB. The sync-source SVM is in the `running` state, and the sync-destination SVM is in the `stopped` state.

What happens during a switchback

After the disaster site has recovered and aggregates have healed, the MetroCluster switchback process returns storage and client access from the disaster recovery site to the home cluster.

The metrocluster switchback command returns the primary site to full, normal MetroCluster operation. Any configuration changes are propagated to the original SVMs. Data server operation is then returned to the sync-source SVMs on the disaster site and the sync-dest SVMs that had been operating on the surviving site are deactivated.

If SVMs were deleted on the surviving site while the MetroCluster configuration was in switchover state, the switchback process does the following:

- Deletes the corresponding SVMs on the partner site (the former disaster site).
- Deletes any peering relationships of the deleted SVMs.

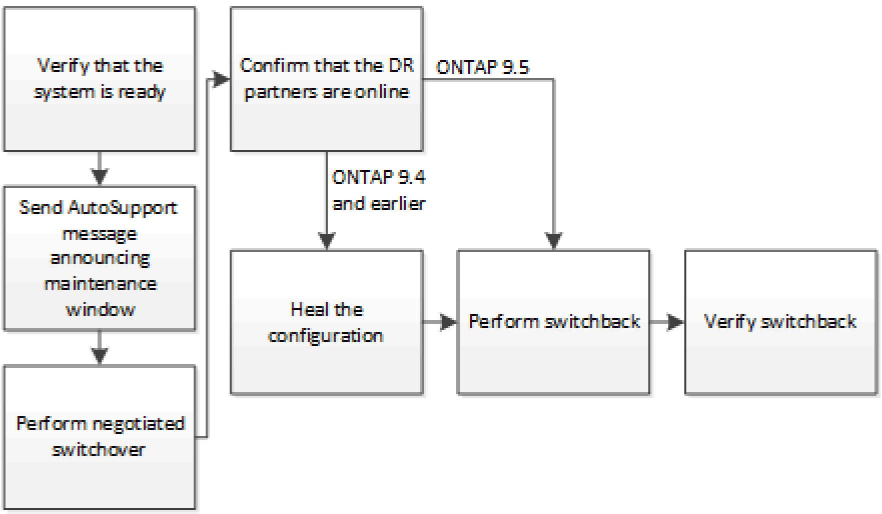
MetroCluster® Management Guide

Preforming switchover, healing, and switchback

This content describes how to perform MetroCluster switchover and switchback operations, both in planned maintenance operations or in the event of a disaster.

Performing switchover for tests or maintenance

If you want to test the MetroCluster functionality or to perform planned maintenance, you can perform a negotiated switchover in which one cluster is cleanly switched over to the partner cluster. You can then heal and switch back the configuration.



Starting with ONTAP 9.6, switchover and switchback operations can be performed on MetroCluster IP configurations with ONTAP System Manager.

Verifying that your system is ready for a switchover

You can use the `-simulate` option to preview the results of a switchover operation. A verification check gives you a way to verify that most of the preconditions for a successful run are met before you start the operation. Issue these commands from the site that will remain up and operational:

1. Set the privilege level to advanced: `set -privilege advanced`
2. From the site that will remain up and operational, simulate a switchover operation: `metrocluster switchover -simulate`
3. Review the output that is returned.

   The output shows whether any vetoes would prevent a switchover operation. Every time you perform a MetroCluster operation, you must verify a set of criteria for the success of the operation. A “veto” is a mechanism to prohibit the operation if one or more of the criteria are not fulfilled. There are two types of veto: a “soft” veto and a “hard” veto. You can override a soft veto, but not a hard veto. For example, to perform a negotiated switchover in a four-node MetroCluster configuration, one criterion is that all of the nodes are up and healthy. Suppose one node is down and was taken over by its HA partner. The switchover operation will be hard vetoed because it is a hard criterion that all of the nodes must be up and healthy. Because this is a hard veto, you cannot override the veto.

> It is best not to override any veto.

Example: Verification results

The following example shows the errors that are encountered in a simulation of a switchover operation:

```
cluster4::*> metrocluster switchover -simulate

[Job 126] Preparing the cluster for the switchover operation...
[Job 126] Job failed: Failed to prepare the cluster for the switchover
operation. Use the "metrocluster operation show" command to view detailed
error
information. Resolve the errors, then try the command again.
```

> Negotiated switchover and switchback will fail until you replace all of the failed disks. You can perform disaster recovery after you replace the failed disks. If you want to ignore the warning for failed disks, you can add a soft veto for the negotiated switchover and switchback.

Sending a custom AutoSupport message prior to negotiated switchover

Before performing a negotiated switchover, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. The negotiated switchover might result in plex or MetroCluster operation failures that trigger AutoSupport messages. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster at Site_A.
2. Invoke an AutoSupport message indicating the start of the maintenance: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

   maintenance-window-in-hours specifies the length of the maintenance window and can be a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can issue a command to indicating that the maintenance period has ended:`system node autosupport invoke -node * -type all -message MAINT=end`
3. Repeat this step on the partner site.

Performing a negotiated switchover

A negotiated switchover cleanly shuts down processes on the partner site, and then switches over operations from the partner site. You can use a negotiated switchover to perform maintenance on a MetroCluster site or to test the switchover functionality.

- All previous configuration changes must be completed before performing a switchback operation.

  This is to avoid competition with the negotiated switchover or switchback operation.

- Any nodes that were previously down must be booted and in cluster quorum.

  The *System Administration Reference* has more information about cluster quorum in the “Understanding quorum and epsilon” section.

  System administration

- The cluster peering network must be available from both sites.
- All of the nodes in the MetroCluster configuration must be running the same version of ONTAP software.
- The option replication.create_data_protection_rels.enable must be set to ON on both of the sites in a MetroCluster configuration before creating a new SnapMirror relationship.
- For a two-node MetroCluster configuration, a new SnapMirror relationship should not be created during an upgrade when there are mismatched versions of ONTAP between the sites.
- For a four-node MetroCluster configuration, the mismatched versions of ONTAP between the sites are not supported.

The recovering site can take a few hours to be able to perform the switchback operation.

The metrocluster switchover command switches over the nodes in all DR groups in the MetroCluster configuration. For example, in an eight-node MetroCluster configuration, it switches over the nodes in both DR groups.

While preparing for and executing a negotiated switchover, you must not make configuration changes to either cluster or perform any takeover or giveback operations.

For MetroCluster FC configurations:

- Mirrored aggregates will remain in normal state if the remote storage is accessible.
- Mirrored aggregates will become degraded after the negotiated switchover if access to the remote storage is lost.
- Unmirrored aggregates that are located at the disaster site will become unavailable if access to the remote storage is lost. This might lead to a controller outage.

For MetroCluster IP configurations:

- For ONTAP 9.4 and earlier:
  - Mirrored aggregates will become degraded after the negotiated switchover.
- For ONTAP 9.5 and later:
  - Mirrored aggregates will remain in normal state if the remote storage is accessible.
  - Mirrored aggregates will become degraded after the negotiated switchover if access to the remote

storage is lost.

* For ONTAP 9.8 and later:
   * Unmirrored aggregates that are located at the disaster site will become unavailable if access to the remote storage is lost. This might lead to a controller outage.

      1. Use the metrocluster check run, metrocluster check show and metrocluster check config-replication show commands to make sure no configuration updates are in progress or pending. Issue these commands from the site that will remain up and operational.
      2. From the site that will remain up and operational, implement the switchover: `metrocluster switchover`

         The operation can take several minutes to complete.
      3. Monitor the completion of the switchover: `metrocluster operation show`

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

      4. Reestablish any SnapMirror or SnapVault configurations.

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.

Confirming that the DR partners have come online

After the switchover is complete, you should verify that the DR partners have taken ownership of the disks and the partner SVMs have come online.

Steps

1. Confirm that the aggregate disks have switched over to the disaster site: `storage disk show -fields owner,dr-home`

In this example, the output shows that the switched over disks have the dr-home field set:

```
cluster_A::> storage disk show -fields owner,dr-home
disk                 owner           dr-home
-------------------- --------------- -------
1.11.0               node_A_1        node_B_1
1.11.1               node_A_1        node_B_1
1.11.2               node_A_1        node_B_1
1.11.3               node_A_1        node_B_1
1.11.4               node_A_1        node_B_1
1.11.5               node_A_1        node_B_1
1.11.6               node_A_1        node_B_1
1.11.7               node_A_1        node_B_1
1.11.8               node_A_1        node_B_1
```

2. Check that the aggregates were switched over by using the storage aggregate show command.

   In this example, the aggregates were switched over. The root aggregate (aggr0_b2) is in a degraded state. The data aggregate (b2_aggr2) is in a mirrored, normal state:

```
cluster_A::*> storage aggregate show

.
.
.
mcc1-b Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b2    227.1GB   45.1GB    80% online       0 node_A_1
raid_dp,

mirror

degraded
b2_aggr1    227.1GB   200.3GB    20% online       0 node_A_1
raid_dp,

mirrored

normal
```

3. Confirm that the secondary SVMs have come online by using the vserver show command.

In this example, the previously dormant sync-destination SVMs on the secondary site have been activated and have an Admin State of running:

```
cluster_A::*> vserver show
                                          Admin      Operational  Root
Name    Name
Vserver          Type  Subtype            State      State        Volume
Aggregate  Service Mapping
-----------      ----- ----------         ---------- -----------
--------- ---------- ------- -------
...
cluster_B-vs1b-mc data   sync-destination  running   running
vs1b_vol   aggr_b1   file    file
```

Healing the configuration

After a negotiated switchover operation, you must perform the healing operations in specific order to restore MetroCluster functionality. The procedure you use depends on the type of MetroCluster configuration you have.

On MetroCluster IP systems running ONTAP 9.5, healing is performed automatically, and you can skip these tasks.

Healing the configuration in a MetroCluster FC configuration

Following a switchover, you must perform the healing operations in specific order to restore MetroCluster functionality.

- Switchover must have been performed and the surviving site must be serving data.
- Nodes on the disaster site must be halted or remain powered off.

  They must not be fully booted during the healing process.
- Storage at the disaster site must be accessible (shelves are powered up, functional, and accessible).
- In fabric-attached MetroCluster configurations, inter-switch links (ISLs) must be up and operating.
- In four-node MetroCluster configurations, nodes in the surviving site must not be in HA failover state (all nodes must be up and running for each HA pair).

The healing operation must first be performed on the data aggregates, and then on the root aggregates.

Healing the data aggregates after negotiated switchover

You must heal the data aggregates after completing any maintenance or testing. This process resynchronizes the data aggregates and prepares the disaster site for normal operation. You must heal the data aggregates prior to healing the root aggregates.

All configuration updates in the remote cluster successfully replicate to the local cluster. You power up the storage on the disaster site as part of this procedure, but you do not and must not power up the controller modules on the disaster site.

Steps

1. Ensure that switchover has been completed by running the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 7/25/2014 20:01:48
   End Time: 7/25/2014 20:02:14
     Errors: -
```

2. Resynchronize the data aggregates by running the metrocluster heal -phase aggregates command from the surviving cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

If the healing is vetoed, you have the option of reissuing the metrocluster heal command with the --override -vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

3. Verify that the operation has been completed by running the metrocluster operation show command.

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. Check the state of the aggregates by running the storage aggregate show command.

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

5. If storage has been replaced at the disaster site, you might need to remirror the aggregates.

Healing the root aggregates after negotiated switchover

After the data aggregates have been healed, you must heal the root aggregates in preparation for the switchback operation.

The data aggregates phase of the MetroCluster healing process must have been completed successfully.

Steps

1. Switch back the mirrored aggregates by running the metrocluster heal -phase root-aggregates command.

   ```
   cluster_A::> metrocluster heal -phase root-aggregates
   [Job 137] Job succeeded: Heal Root Aggregates is successful
   ```

   If the healing is vetoed, you have the option of reissuing the metrocluster heal command with the --override -vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

2. Confirm the heal operation is complete by running the metrocluster operation show command on the healthy cluster:

   ```
   cluster_A::> metrocluster operation show
     Operation: heal-root-aggregates
         State: successful
    Start Time: 7/29/2014 20:54:41
      End Time: 7/29/2014 20:54:42
        Errors: -
   ```

3. Check for and remove any failed disks belonging to the disaster site by issuing the following command on the healthy site: `disk show -broken`
4. Power up or boot each controller module on the disaster site.

   If the system displays the LOADER prompt, run the `boot_ontap` command.

5. After nodes are booted, verify that the root aggregates are mirrored.

   If both plexes are present, resynchronization will occur automatically if the plexes are not synchronized. If one plex has failed, that plex must be destroyed and the mirror must be recreated using the storage aggregate mirror -aggregateaggregate-name command to reestablish the mirror relationship.

Healing the configuration in a MetroCluster IP configuration (ONTAP 9.4 and earlier)

You must heal the aggregates in preparation for the switchback operation.

The following conditions must exist before performing the healing procedure:

- Switchover must have been performed and the surviving site must be serving data.
- Storage shelves at the disaster site must be powered up, functional, and accessible.

- ISLs must be up and operating.
- Nodes in the surviving site must not be in HA failover state (both nodes must be up and running).

This task applies to MetroCluster IP configurations running ONTAP versions prior to 9.5 only.

This procedure differs from the healing procedure for MetroCluster FC configurations.

Steps

1. Power up each controller module on the site that was switched over and let them fully boot.

   If the system displays the LOADER prompt, run the `boot_ontap` command.

2. Perform the root aggregate healing phase: `metrocluster heal root-aggregates`

   ```
   cluster_A::> metrocluster heal root-aggregates
   [Job 137] Job succeeded: Heal Root-Aggregates is successful
   ```

   If the healing is vetoed, you have the option of reissuing the metrocluster heal root-aggregates command with the --override-vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

3. Resynchronize the aggregates: `metrocluster heal aggregates`

   ```
   cluster_A::> metrocluster heal aggregates
   [Job 137] Job succeeded: Heal Aggregates is successful
   ```

   If the healing is vetoed, you have the option of reissuing the metrocluster heal command with the --override -vetoes parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

4. Confirm the heal operation is complete by running the metrocluster operation show command on the healthy cluster:

   ```
   cluster_A::> metrocluster operation show
     Operation: heal-aggregates
         State: successful
    Start Time: 7/29/2017 20:54:41
      End Time: 7/29/2017 20:54:42
        Errors: -
   ```

Performing a switchback

After you heal the MetroCluster configuration, you can perform the MetroCluster switchback operation. The MetroCluster switchback operation returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the disaster site active and serving data from the local disk pools.

- The disaster cluster must have successfully switched over to the surviving cluster.
- Healing must have been performed on the data and root aggregates.
- The surviving cluster nodes must not be in the HA failover state (all nodes must be up and running for each HA pair).
- The disaster site controller modules must be completely booted and not in the HA takeover mode.
- The root aggregate must be mirrored.
- The Inter-Switch Links (ISLs) must be online.
- Any required licenses must be installed on the system.

1. Confirm that all nodes are in the enabled state: `metrocluster node show`

   The following example displays the nodes that are in the enabled state:

```
cluster_B::>  metrocluster node show

DR                          Configuration  DR
Group Cluster Node          State          Mirroring Mode
----- ------- ----------- -------------- ---------
--------------------
1     cluster_A
              node_A_1     configured     enabled   heal roots
completed
              node_A_2     configured     enabled   heal roots
completed
      cluster_B
              node_B_1     configured     enabled   waiting for
switchback recovery
              node_B_2     configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Confirm that resynchronization is complete on all SVMs: `metrocluster vserver show`
3. Verify that any automatic LIF migrations being performed by the healing operations have been successfully completed: metrocluster check lif show
4. Perform the switchback by running the metrocluster switchback command from any node in the surviving cluster: `metrocluster switchback`
5. Check the progress of the switchback operation: `metrocluster show`

   The switchback operation is still in progress when the output displays waiting-for-switchback:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

The switchback operation is complete when the output displays normal:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

If a switchback takes a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command. This command is at the advanced privilege level.

6. Reestablish any SnapMirror or SnapVault configurations.

   In ONTAP 8.3, you need to manually reestablish a lost SnapMirror configuration after a MetroCluster switchback operation. In ONTAP 9.0 and later, the relationship is reestablished automatically.

Verifying a successful switchback

After performing the switchback, you want to confirm that all aggregates and storage virtual machines (SVMs) are switched back and online.

1. Verify that the switched-over data aggregates are switched back: `storage aggregate show`

   In the following example, aggr_b2 on node B2 has switched back:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

If the disaster site included unmirrored aggregates and the unmirrored aggregates are no longer present, the aggregate may show up with a State of unknown in the output of the storage aggregate show command. Contact technical support to remove the out-of-date entries for the unmirrored aggregates.

2. Verify that all sync-destination SVMs on the surviving cluster are dormant (showing an Admin State of stopped) and the sync-source SVMs on the disaster cluster are up and running: `vserver show -subtype sync-source`

```
node_B_1::> vserver show -subtype sync-source
                               Admin      Root
Name    Name
Vserver     Type    Subtype    State      Volume     Aggregate
Service Mapping
----------- ------- ---------- ---------- ---------- ----------
------- -------
...
vs1a        data    sync-source
                               running    vs1a_vol   node_B_2
file    file

aggr_b2

node_A_1::> vserver show -subtype sync-destination
                               Admin      Root
Name    Name
Vserver            Type    Subtype    State      Volume     Aggregate
Service Mapping
-----------        ------- ---------- ---------- ---------- ----------
------- -------
...
cluster_A-vs1a-mc  data    sync-destination
                                      stopped    vs1a_vol   sosb_
file    file

aggr_b2
```

Sync-destination aggregates in the MetroCluster configuration have the suffix "-mc" automatically appended to their name to help identify them.

3. Confirm that the switchback operations succeeded by using the metrocluster operation show command.

If the command output shows…	Then…
That the switchback operation state is successful.	The switchback process is complete and you can proceed with operation of the system.
That the switchback operation or switchback-continuation-agent operation is partially successful.	Perform the suggested fix provided in the output of the metrocluster operation show command.

You must repeat the previous sections to perform the switchback in the opposite direction. If site_A did a switchover of site_B, have site_B do a switchover of site_A.

Commands for switchover, healing, and switchback

There are specific ONTAP commands for performing the MetroCluster disaster recovery processes.

If you want to…	Use this command…
Verify that switchover can be performed without errors or vetoes.	`metrocluster switchover -simulate` at the advanced privilege level
Verify that switchback can be performed without errors or vetoes.	`metrocluster switchback -simulate` at the advanced privilege level
Switch over to the partner nodes (negotiated switchover).	`metrocluster switchover`
Switch over to the partner nodes (forced switchover).	`metrocluster switchover -forced-on -disaster true`
Perform data aggregate healing.	`metrocluster heal -phase aggregates`
Perform root aggregate healing.	`metrocluster heal -phase root-aggregates`
Switch back to the home nodes.	`metrocluster switchback`

Monitoring the MetroCluster configuration

You can use ONTAP MetroCluster commands and Active IQ Unified Manager (formerly OnCommand Unified Manager) to monitor the health of a variety of software components and the state of MetroCluster operations.

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
```

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"
```

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.

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

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr1
```

```
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                       controller_A_1_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok


controller_A_2         controller_A_2_aggr0
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                       controller_A_2_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                       controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

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

Cluster               Check                              Result
--------------------- ------------------------------- ---------
mccint-fas9000-0102
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
mccint-fas9000-0304
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
10 entries were displayed.
```

Commands for checking and monitoring the MetroCluster configuration

There are specific ONTAP commands for monitoring the MetroCluster configuration and checking MetroCluster operations.

Commands for checking MetroCluster operations

If you want to…	Use this command…
Perform a check of the MetroCluster operations. **Note:** This command should not be used as the only command for pre-DR operation system validation.	`metrocluster check run`
View the results of the last check on MetroCluster operations.	`metrocluster show`
View results of check on configuration replication between the sites.	`metrocluster check config-replication show metrocluster check config-replication show-aggregate-eligibility`
View results of check on node configuration.	`metrocluster check node show`
View results of check on aggregate configuration.	`metrocluster check aggregate show`
View the LIF placement failures in the MetroCluster configuration.	`metrocluster check lif show`

Commands for monitoring the MetroCluster interconnect

If you want to…	Use this command…
Display the HA and DR mirroring status and information for the MetroCluster nodes in the cluster.	`metrocluster interconnect mirror show`

Commands for monitoring MetroCluster SVMs

If you want to…	Use this command…
View all SVMs in both sites in the MetroCluster configuration.	`metrocluster vserver show`

Using the MetroCluster Tiebreaker or ONTAP Mediator to monitor the configuration

See Differences between ONTAP Mediator and MetroCluster Tiebreaker to understand the differences between these two methods of monitoring your MetroCluster configuration and initiating an automatic switchover.

Use these links to install and configure Tiebreaker or Mediator:

- Install and configure the MetroCluster Tiebreaker software
- Configure the ONTAP Mediator service for unplanned automatic switchover

How the NetApp MetroCluster Tiebreaker software detects failures

The Tiebreaker software resides on a Linux host. You need the Tiebreaker software only if you want to monitor 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, from a site failure.

After you install the Tiebreaker software on a Linux host, you can configure the clusters in a MetroCluster configuration to monitor for disaster conditions.

How the Tiebreaker software detects intersite connectivity failures

The MetroCluster Tiebreaker software alerts you if all connectivity between the sites is lost.

Types of network paths

Depending on the configuration, there are three types of network paths between the two clusters in a MetroCluster configuration:

- **FC network (present in fabric-attached MetroCluster configurations)**

  This type of network is composed of two redundant FC switch fabrics. Each switch fabric has two FC switches, with one switch of each switch fabric co-located with a cluster. Each cluster has two FC switches, one from each switch fabric. All of the nodes have FC (NV interconnect and FCP initiator) connectivity to each of the co-located IP switches. Data is replicated from cluster to cluster over the ISL.

- **Intercluster peering network**

  This type of network is composed of a redundant IP network path between the two clusters. The cluster peering network provides the connectivity that is required to mirror the storage virtual machine (SVM) configuration. The configuration of all of the SVMs on one cluster is mirrored by the partner cluster.

- **IP network (present in MetroCluster IP configurations)**

  This type of network is composed of two redundant IP switch networks. Each network has two IP switches, with one switch of each switch fabric co-located with a cluster. Each cluster has two IP switches, one from each switch fabric. All of the nodes have connectivity to each of the co-located FC switches. Data is replicated from cluster to cluster over the ISL.

Monitoring intersite connectivity

The Tiebreaker software regularly retrieves the status of intersite connectivity from the nodes. If NV interconnect connectivity is lost and the intercluster peering does not respond to pings, then the clusters assume that the sites are isolated and the Tiebreaker software triggers an alert as "AllLinksSevered". If a cluster identifies the "AllLinksSevered" status and the other cluster is not reachable through the network, then the Tiebreaker software triggers an alert as "disaster".

How the Tiebreaker software detects site failures

The NetApp MetroCluster Tiebreaker software checks the reachability of the nodes in a MetroCluster configuration and the cluster to determine whether a site failure has occurred. The Tiebreaker software also triggers an alert under certain conditions.

Components monitored by the Tiebreaker software

The Tiebreaker software monitors each controller in the MetroCluster configuration by establishing redundant connections through multiple paths to a node management LIF and to the cluster management LIF, both hosted on the IP network.

The Tiebreaker software monitors the following components in the MetroCluster configuration:

- Nodes through local node interfaces
- Cluster through the cluster-designated interfaces
- Surviving cluster to evaluate whether it has connectivity to the disaster site (NV interconnect, storage, and intercluster peering)

When there is a loss of connection between the Tiebreaker software and all of the nodes in the cluster and to the cluster itself, the cluster will be declared as “not reachable” by the Tiebreaker software. It takes around three to five seconds to detect a connection failure. If a cluster is unreachable from the Tiebreaker software, the surviving cluster (the cluster that is still reachable) must indicate that all of the links to the partner cluster are severed before the Tiebreaker software triggers an alert.

> All of the links are severed if the surviving cluster can no longer communicate with the cluster at the disaster site through FC (NV interconnect and storage) and intercluster peering.

Failure scenarios during which Tiebreaker software triggers an alert

The Tiebreaker software triggers an alert when the cluster (all of the nodes) at the disaster site is down or unreachable and the cluster at the surviving site indicates the "AllLinksSevered" status.

The Tiebreaker software does not trigger an alert (or the alert is vetoed) in the following scenarios:

- In an eight-node MetroCluster configuration, if one HA pair at the disaster site is down
- In a cluster with all of the nodes at the disaster site down, one HA pair at the surviving site down, and the cluster at the surviving site indicates the "AllLinksSevered" status

  The Tiebreaker software triggers an alert, but ONTAP vetoes that alert. In this situation, a manual switchover is also vetoed
- Any scenario in which the Tiebreaker software can either reach at least one node or the cluster interface at the disaster site, or the surviving site still can reach either node at the disaster site through either FC (NV interconnect and storage) or intercluster peering

How the ONTAP Mediator supports automatic unplanned switchover

The ONTAP Mediator stores state information about the MetroCluster nodes in mailboxes located on the Mediator host. The MetroCluster nodes can use this information to monitor the state of their DR partners and implement a Mediator-assisted automatic unplanned switchover (MAUSO) in the case of a disaster.

When a node detects a site failure requiring a switchover, it takes steps to confirm that the switchover is appropriate and, if so, performs the switchover.

MAUSO is only initiated if both SyncMirror mirroring and DR mirroring of each node’s nonvolatile cache is operating and the caches and mirrors are synchronized at the time of the failure.

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:

If…	Then…
ONTAP detects no NVRAM errors	File service starts normally.
ONTAP detects NVRAM errors	• ONTAP returns a stale file handle (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 `in-nvfailed-state` option on the affected volume.
If one of the following parameters is used: • `dr-force-nvfail` volume option is set • `force-nvfail-all` switchover command option is set.	You can unset the `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 `in-nvfailed-state` option on the affected volume. Using the `force-nvfail-all` option causes the `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 `in-nvfailed-state` option on the volume must be cleared, and the 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 backup as necessary. After all of the LUNs in the volume are recovered, the `in-nvfailed-state` option on the affected volume is cleared.

Commands for monitoring data loss events

If you enable the 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.

If you want to…	Use this command…
Create a new volume with NVFAIL enabled	`volume create -nvfail on`
Enable NVFAIL on an existing volume	`volume modify` **Note:** You set the `-nvfail` option to "on" to enable NVFAIL on the created volume.
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.

Related information

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.

Related information

Monitoring and protecting the files system consistency using NVFAIL

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.

Where to find additional information

You can learn more about MetroCluster configuration and operation in NetApp's extensive documentation library.

MetroCluster and miscellaneous guides

Guide	Content
ONTAP 9 Documentation Center	• All MetroCluster guides
NetApp Technical Report 4375: NetApp MetroCluster for ONTAP 9.3	• A technical overview of the MetroCluster configuration and operation. • Best practices for MetroCluster 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
Stretch MetroCluster installation and configuration	• Stretch MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • Configuring the MetroCluster in ONTAP

Guide	Content
MetroCluster IP installation and configuration	• MetroCluster IP architecture • Cabling the configuration • Configuring the MetroCluster in ONTAP
MetroCluster Tiebreaker 1.21 software installation and configuration	• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software
Active IQ Unified Manager documentation NetApp Documentation: Product Guides and Resources	• Monitoring the MetroCluster configuration and performance
Copy-based transition	• Transitioning data from 7-Mode storage systems to clustered storage systems

Maintain the MetroCluster components

Where to find procedures for MetroCluster maintenance tasks

You should be sure you select the correct procedure when you perform MetroCluster hardware maintenance tasks.

> With the release of ONTAP 9.8, the MetroCluster upgrade and expansion procedures have moved to the MetroCluster Upgrade and Expansion Guide and MetroCluster Transition Guide.

Component	MetroCluster type (FC or IP)	Task	Procedure
ONTAP software	Both	ONTAP software upgrade	Upgrade, revert, or downgrade
Controller module	Both	FRU replacement (including controller modules, PCIe cards, FC-VI card, and so on) Moving a storage controller module or NVRAM card among the MetroCluster storage systems is not supported.	AFF and FAS Documentation Center
		Upgrade and expansion	MetroCluster® Upgrade and Expansion Guide
		Transition from FC to IP connectivity	MetroCluster® Transition Guide

Component	MetroCluster type (FC or IP)	Task	Procedure
Drive shelf	FC	Shelf addition (stack with bridges or individual shelf)	Hot-adding a stack of SAS disk shelves to an existing pair of FibreBridge 7500N bridges Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system Hot-adding a SAS disk shelf to a stack of SAS disk shelves
	FC	Shelf removal	Hot-removing storage from a MetroCluster FC configuration
	FC	All other shelf maintenance procedures. The standard procedures can be used.	Service Guide for DS460C DS224C and DS212C Disk Shelves
	IP	All shelf maintenance procedures. The standard procedures can be used. If adding shelves for an unmirrored aggregate, see Considerations when using unmirrored aggregates	Service Guide for DS460C DS224C and DS212C Disk Shelves
	Both	Hot adding IOM12 shelves to a stack of IOM6 shelves	Hot-adding shelves with IOM12 modules to a stack of shelves with IOM6 modules

Component	MetroCluster type (FC or IP)	Task	Procedure
FC-to-SAS bridge	FC	Bridge replacement	Replacing a single FC-to-SAS bridge Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges Hot-swapping a FibreBridge 7500N with a 7600N bridge
	FC	Firmware upgrade	Updating the firmware on a FibreBridge bridge
	FC	Replacing a failed power supply module	Hot-replacing a failed power supply module
FC switch	FC	Switch upgrade	Upgrading to new Brocade FC switches
	FC	Switch replacement	Replacing a Brocade FC switch (MetroCluster) Replacing a Cisco FC switch
	FC	Firmware upgrade	Updating firmware on a Brocade FC switch Updating firmware on a Cisco FC switch

MetroCluster failure and recovery scenarios

You should be aware of how the MetroCluster configuration responds to different failure events.

For additional information about recovery from node failures, see the section "Choosing the correct recovery procedure" in the MetroCluster Management and Disaster Recovery Guide.

Event	Impact	Recovery
Single node failure	A failover is triggered.	The configuration recovers through a local takeover. RAID is not impacted. Review system messages and replace failed FRUs as necessary. AFF and FAS Documentation Center
Two nodes fail at one site	Two nodes will fail only if automated switchover is enabled in the MetroCluster Tiebreaker software.	Manual USO if automated switchover in MetroCluster Tiebreaker software is not enabled. AFF and FAS Documentation Center
MetroCluster IP interface—failure of one port	The system is degraded. Additional port failure impacts HA mirroring.	The second port is used. Health Monitor generates an alert if the physical link to the port is broken. Review system messages and replace failed FRUs as necessary. AFF and FAS Documentation Center
MetroCluster IP interface—failure of both ports	HA capability is impacted. RAID SyncMirror of the node stops syncing.	Immediate manual recovery is required as there is no HA takeover. Review system messages and replace failed FRUs as necessary. AFF and FAS Documentation Center
Failure of one MetroCluster IP switch	No impact. Redundancy is provided through the second network.	Replace the failed switch as necessary. Replacing an IP switch
Failure of two MetroCluster IP switches that are in the same network	No impact. Redundancy is provided through the second network.	Replace the failed switch as necessary. Replacing an IP switch
Failure of two MetroCluster IP switches that are at one site	RAID SyncMirror of the node stops syncing. HA capability is impacted and the cluster goes out of quorum.	Replace the failed switch as necessary. Replacing an IP switch

Event	Impact	Recovery
Failure of two MetroCluster IP switches that are at different sites and not on the same network (diagonal failure)	RAID SyncMirror of the node stops syncing.	RAID SyncMirror of the node stops syncing. Cluster and HA capability are not impacted. Replace the failed switch as necessary. Replacing an IP switch

Performing FC-to-SAS bridge maintenance

If necessary, you can nondisruptively replace the FC-to-SAS bridges or upgrade their firmware in the MetroCluster configuration.

FibreBridge 6500N bridges are not supported in configurations running ONTAP 9.8 and later.

Support for FibreBridge 7600N bridges in MetroCluster configurations

The FibreBridge 7600N bridge is supported on ONTAP 9.5 and later as a replacement for the FibreBridge 7500N or 6500N bridge or when adding new storage to the MetroCluster configuration. The zoning requirements and restrictions regarding use of the bridge’s FC ports are the same as that of the FibreBridge 7500N bridge.

NetApp Interoperability Matrix Tool

FibreBridge 6500N bridges are not supported in configurations running ONTAP 9.8 and later.

Use case	Zoning changes needed?	Restrictions	Procedure
Replacing a single FibreBridge 7500N bridge with a single FibreBridge 7600N bridge	No	The FibreBridge 7600N bridge must be configured exactly the same as the FibreBridge 7500N bridge.	Hot-swapping a FibreBridge 7500N with a 7600N bridge
Replacing a single FibreBridge 6500N bridge with a single FibreBridge 7600N bridge	No	The FibreBridge 7600N bridge must be configured exactly the same as the FibreBridge 6500N bridge.	Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge

Use case	Zoning changes needed?	Restrictions	Procedure
Adding new storage through adding a new pair of FibreBridge 7600N bridges	YesYou must add storage zones for each of the FC ports of the new bridges.	You must have available ports on the FC switch fabric (in a fabric-attached MetroCluster configuration) or on the storage controllers (in a stretch MetroCluster configuration).Each pair of FibreBridge 7500N or 7600N bridges can support up to four stacks.	Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system

Support for FibreBridge 7500N bridges in MetroCluster configurations

The FibreBridge 7500N bridge is supported as a replacement for the FibreBridge 6500N bridge or for when adding new storage to the MetroCluster configuration. The supported configurations have zoning requirements and restrictions regarding use of the bridge’s FC ports and stack and storage shelf limits.

FibreBridge 6500N bridges are not supported in configurations running ONTAP 9.8 and later.

Use case	Zoning changes needed?	Restrictions	Procedure
Replacing a single FibreBridge 6500N bridge with a single FibreBridge 7500N bridge	No	The FibreBridge 7500N bridge must be configured exactly the same as the FibreBridge 6500N bridge, using a single FC port and attaching to a single stack. The second FC port on the FibreBridge 7500N must not be used.	Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge

Use case	Zoning changes needed?	Restrictions	Procedure
Consolidating multiple stacks by replacing multiple pairs of FibreBridge 6500N bridges with a single pair of FibreBridge 7500N bridges	Yes	In this case, you take the FibreBridge 6500N bridges out of service and replace them with a single pair of FibreBridge 7500N bridges.Each pair of FibreBridge 7500N or 7600N bridges can support up to four stacks. At the end of the procedure, both the top and bottom of the stacks must be connected to corresponding ports on the FibreBridge 7500N bridges.	Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges
Adding new storage through adding a new pair of FibreBridge 7500N bridges	YesYou must add storage zones for each of the FC ports of the new bridges.	You must have available ports on the FC switch fabric (in a fabric-attached MetroCluster configuration) or on the storage controllers (in a stretch MetroCluster configuration).Each pair of FibreBridge 7500N or 7600N bridges can support up to four stacks.	Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system

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.

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.

Starting with ONTAP 9.8, *in-band management* of the bridges is supported by default and out-of-band SNMP management is deprecated.

This task is required if you are **not** using in-band management to manage the bridges. In this case, 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 a service, if desired, by issuing the `set closeport` and repeating the command as necessary until all desired services are disabled:

   `set closeport` *`service`*

   The `set closeport` command disables a single service at a time.

   `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.
4. If you are enabling SNMP, you must also issue the set SNMP enabled command:

   `set SNMP enabled`

   SNMP is the only protocol that requires a separate enable command.

5. Save the configuration:

   `saveconfiguration`

Updating firmware on a FibreBridge bridge

The procedure for updating the bridge firmware depends on your bridge model and ONTAP version.

Updating firmware on FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later

You might need to update the firmware on your FibreBridge bridges to ensure that you have the latest features or to resolve possible issues. This procedure should be used for FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later.

- The MetroCluster configuration must be operating normally.
- All of the FibreBridge bridges in the MetroCluster configuration must be up and operating.
- All of the storage paths must be available.
- You need the admin password and access to an HTTP server.
- You must be using a supported firmware version.

  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.

- You can use this task only on FibreBridge 7600N or 7500N bridges in configurations running ONTAP 9.4 or later.
- You must perform this task on each FibreBridge bridge in the MetroCluster configuration, so that all of the bridges are running the same firmware version.

> This procedure is nondisruptive and takes approximately 30 minutes to complete.

> Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

Steps

1. Invoke an AutoSupport message indicating the start of the maintenance:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   maintenance-window-in-hours specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

   `system node autosupport invoke -node * -type all -message MAINT=end`

2. Go to the ATTO FibreBridge page and select the appropriate firmware for your bridge.

   ATTO FibreBridge Firmware Download Page

3. Review the Caution/MustRead and End User Agreement, and click the check box to indicate acceptance and proceed.
4. Place the firmware file in a network location that is network accessible to the controller modules.

   You can enter the commands in the remaining steps from the console of either controller module.

5. Change to the advanced privilege level:

   `set -privilege advanced`

   You must respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

6. Update the bridge firmware by using the following command:

   `storage bridge firmware update -bridge name -uri` ***`URL-of-firmware-package`***

   ```
   cluster_A> storage bridge firmware update -bridge bridge_A_1a -uri
   http://192.168.132.97/firmware.spf
   ```

7. Return to the admin privilege level:

   `set -privilege admin`

8. Verify that the firmware upgrade is complete:

   `job show -name "`*`job-name`*`"`

   The following example shows that the job **storage bridge firmware update** is still running:

   ```
   cluster_A> job show -name "storage bridge firmware update"
   Owning

   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   2246   job-name
                               cluster_A
                                          node_A_1
                                                         Running
   Description: Storage bridge firmware update job
   ```

   After approximately 10 minutes, the new firmware is fully installed and the job state will be Success:

   ```
   cluster_A> job show -name "storage bridge firmware update"

                               Owning
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   2246   Storage bridge firmware update
                               cluster_A
                                          node_A_1
                                                         Success
   Description: Storage bridge firmware update job
   ```

9. Complete the steps according to whether in-band management is enabled and which version of ONTAP your system is running:

◦ If you are running ONTAP 9.4, in-band management is not supported and the command must be issued from the bridge console:

i. Run the **`flashimages`** command on the console of the bridge and confirm that the correct firmware versions are displayed.

> The example shows that primary flash image shows the new firmware image, while the secondary flash image shows the old image.

```
flashimages

 ;Type Version
;=====================================================
Primary 3.16 001H
Secondary 3.15 002S
Ready.
```

i. Reboot the bridge by running the **`firmwarerestart`** command from the bridge.

▪ If you are running ONTAP 9.5 or later, in-band management is supported and the command can be issued from the cluster prompt:

ii. Run the **`storage bridge run-cli -name`** ***`bridge-name`*** **`-command FlashImages`** command.

> The example shows that primary flash image shows the new firmware image, while the secondary flash image shows the old image.

```
cluster_A> storage bridge run-cli -name ATTO_7500N_IB_1 -command
FlashImages

[Job 2257]

;Type         Version
;=====================================================
Primary 3.16 001H
Secondary 3.15 002S
Ready.


[Job 2257] Job succeeded.
```

iii. If necessary, restart the bridge: **`storage bridge run-cli -name ATTO_7500N_IB_1 -command FirmwareRestart`**

> Starting with ATTO firmware version 2.95 the bridge will restart automatically and this step is not required.

10. Verify that the bridge restarted correctly:

    sysconfig

    The system should be cabled for multipath high availability (both controllers have access through the bridges to the disk shelves in each stack).

    ```
    cluster_A> node run -node cluster_A-01 -command sysconfig
    NetApp Release 9.6P8: Sat May 23 16:20:55 EDT 2020
    System ID: 1234567890 (cluster_A-01); partner ID: 0123456789 (cluster_A-
    02)
    System Serial Number: 200012345678 (cluster_A-01)
    System Rev: A4
    System Storage Configuration: Quad-Path HA
    ```

11. Verify that the FibreBridge firmware was updated:

    storage bridge show -fields fw-version,symbolic-name

    ```
    cluster_A> storage bridge show -fields fw-version,symbolic-name
    name fw-version symbolic-name
    ----------------- ----------------- -------------
    ATTO_20000010affeaffe 3.10 A06X bridge_A_1a
    ATTO_20000010affeffae 3.10 A06X bridge_A_1b
    ATTO_20000010affeafff 3.10 A06X bridge_A_2a
    ATTO_20000010affeaffa 3.10 A06X bridge_A_2b
    4 entries were displayed.
    ```

12. Verify the partitions are updated from the bridge's prompt:

    flashimages

    The primary flash image displays the new firmware image, while the secondary flash image displays the old image.

    ```
    Ready.
    flashimages

    ;Type         Version
    ;=====================================================
       Primary    3.16 001H
     Secondary    3.15 002S

     Ready.
    ```

13. Repeat steps 5 to 10 to ensure that both flash images are updated to the same version.
14. Verify that both flash images are updated to the same version.

    `flashimages`

    The output should show the same version for both partitions.

```
Ready.
flashimages

;Type         Version
;=====================================================
   Primary    3.16 001H
 Secondary    3.16 001H

 Ready.
```

15. Repeat steps 5 to 13 on the next bridge until all of the bridges in the MetroCluster configuration have been updated.

Updating firmware on FibreBridge 7500N on configurations running ONTAP 9.3.x and earlier or 6500N bridges

You might need to update the firmware on your FibreBridge bridges to ensure that you have the latest features or to resolve possible issues. This procedure should be used for FibreBridge 7500N on configurations running ONTAP 9.3.x or for FibreBridge 6500N bridges on all supported versions of ONTAP.

- The MetroCluster configuration must be operating normally.
- All of the FibreBridge bridges in the MetroCluster configuration must be up and operating.
- All of the storage paths must be available.
- You need the admin password and access to an FTP or SCP server.
- You must be using a supported firmware version.

  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.

You can use this task with either FibreBridge 7500N or 6500N bridges. Starting with ONTAP 9.3, you can use the ONTAP storage bridge firmware update command to update bridge firmware on FibreBridge 7500N bridges.

Updating firmware on FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later

You must perform this task on each FibreBridge bridge in the MetroCluster configuration, so that all of the bridges are running the same firmware version.

This procedure is nondisruptive and takes approximately 30 minutes to complete.

Steps

1. Invoke an AutoSupport message indicating the start of the maintenance:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   `maintenance-window-in-hours` specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

   `system node autosupport invoke -node * -type all -message MAINT=end`

2. Go to the ATTO FibreBridge page and select the appropriate firmware for your bridge.

   ATTO FibreBridge Firmware Download Page

3. Review the Caution/MustRead and End User Agreement, and click the check box to indicate acceptance and proceed.
4. Download the bridge firmware file using Steps 1 through 3 of the procedure on the ATTO FibreBridge Firmware Download page.
5. Make a copy of the ATTO FibreBridge Firmware Download page and release notes for reference when you are instructed to update the firmware on each bridge.
6. Update the bridge:
   a. Install the firmware on the FibreBridge bridge.
      - If you are using ATTO FibreBridge 7500N bridges, you should refer to the instructions provided in the "Update Firmware" section of the *ATTO FibreBridge 7500N Installation and Operation Manual*.
      - If you are using ATTO FibreBridge 6500N bridges, you should refer to the instructions provided in the "Update Firmware" section of the *ATTO FibreBridge 6500N Installation and Operation Manual*. **ATTENTION:** You should be sure to power-cycle the individual bridge now. If you wait and power-cycle both bridges in a stack simultaneously, the controller might lose access to the drives, resulting in a plex failure or multidisk panic.

        The bridge should restart.

   b. From the console of either controller, verify that the bridge restarted correctly:
      `sysconfig`

      The system should be cabled for multipath high availability (both controllers have access through the bridges to the disk shelves in each stack).

```
cluster_A::> node run -node cluster_A-01 -command sysconfig
NetApp Release 9.1P7: Sun Aug 13 22:33:49 PDT 2017
System ID: 1234567890 (cluster_A-01); partner ID: 0123456789
(cluster_A-02)
System Serial Number: 200012345678 (cluster_A-01)
System Rev: A4
System Storage Configuration: Quad-Path HA
```

c. From the console of either controller, verify that the FibreBridge firmware was updated:
`storage bridge show -fields fw-version,symbolic-name`

```
cluster_A::> storage bridge show -fields fw-version,symbolic-name
 name              fw-version        symbolic-name
 ----------------- ----------------- -------------
 ATTO_10.0.0.1     1.63 071C 51.01   bridge_A_1a
 ATTO_10.0.0.2     1.63 071C 51.01   bridge_A_1b
 ATTO_10.0.1.1     1.63 071C 51.01   bridge_B_1a
 ATTO_10.0.1.2     1.63 071C 51.01   bridge_B_1b
 4 entries were displayed.
```

d. Repeat the previous substeps on the same bridge to update the second partition.

e. Verify that both partitions are updated:
`flashimages`

The output should show the same version for both partitions.

```
Ready.
flashimages
4
;Type         Version
;=====================================================
Primary    2.80 003T
Secondary    2.80 003T
Ready.
```

7. Repeat the previous step on the next bridge, until all of the bridges in the MetroCluster configuration have been updated.

Replacing a single FC-to-SAS bridge

You can nondisruptively replace a bridge with a same model bridge or with a new model bridge.

You need the admin password and access to an FTP or SCP server.

This procedure is nondisruptive and takes approximately 60 minutes to complete.

This procedure uses the bridge CLI to configure and manage a bridge, and to update the bridge firmware and the ATTO QuickNAV utility to configure the bridge Ethernet management 1 port. You can use other interfaces if they meet the requirements.

Requirements for using other interfaces to configure and manage FibreBridge bridges

Related information

Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges

Verifying storage connectivity

Before replacing bridges, you should verify bridge and storage connectivity. Familiarizing yourself with the command output enables you to subsequently confirm connectivity after making configuration changes.

You can issue these commands from the admin prompt of any of the controller modules in the MetroCluster configuration at the site undergoing maintenance.

Steps

1. Confirm connectivity to the disks by entering the following command on any one of the MetroCluster nodes:

   `run local sysconfig -v`

   The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
```

```
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Hot-swapping a bridge with a replacement bridge of the same model

You can hot-swap a failed bridge with another bridge of the same model.

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.

> Starting with ONTAP 9.8, the **`storage bridge`** command is replaced with **`system bridge`**. The following steps show the **`storage bridge`** command, but if you are running ONTAP 9.8 or later, the **`system bridge`** command is preferred.

Steps

1. If the old bridge is accessible, you can retrieve the configuration information.

If…	Then…
You are using IP management	Connect to the old bridge with a Telnet connection and copy the output of the bridge configuration.
You are using in-band management	Use the ONTAP CLI to retrieve the configuration information with the following commands: **`storage bridge run-cli -name *bridge-name* -command "info"`** **`storage bridge run-cli -name *bridge-name* -command "sasportlist"`**

Enter the command:

`storage bridge run-cli -name bridge_A1 -command "info"`

```
info

Device Status          = Good
Unsaved Changes        = None
Device                 = "FibreBridge 7500N"
Serial Number          = FB7500N100000
Device Version         = 3.10
Board Revision         = 7
Build Number           = 007A
Build Type             = Release
Build Date             = "Aug 20 2019" 11:01:24
Flash Revision         = 0.02
Firmware Version       = 3.10
BCE Version (FPGA 1)   = 15
BAU Version (FPGA 2)   = 33
User-defined name      = "bridgeA1"
World Wide Name        = 20 00 00 10 86 A1 C7 00
MB of RAM Installed    = 512
FC1 Node Name          = 20 00 00 10 86 A1 C7 00
FC1 Port Name          = 21 00 00 10 86 A1 C7 00
FC1 Data Rate          = 16Gb
FC1 Connection Mode    = ptp
FC1 FW Revision        = 11.4.337.0
FC2 Node Name          = 20 00 00 10 86 A1 C7 00
FC2 Port Name          = 22 00 00 10 86 A1 C7 00
FC2 Data Rate          = 16Gb
FC2 Connection Mode    = ptp
```

```
FC2 FW Revision        = 11.4.337.0
SAS FW Revision        = 3.09.52
MP1 IP Address         = 10.10.10.10
MP1 IP Subnet Mask     = 255.255.255.0
MP1 IP Gateway         = 10.10.10.1
MP1 IP DHCP            = disabled
MP1 MAC Address        = 00-10-86-A1-C7-00
MP2 IP Address         = 0.0.0.0 (disabled)
MP2 IP Subnet Mask     = 0.0.0.0
MP2 IP Gateway         = 0.0.0.0
MP2 IP DHCP            = enabled
MP2 MAC Address        = 00-10-86-A1-C7-01
SNMP                   = enabled
SNMP Community String = public
PS A Status            = Up
PS B Status            = Up
Active Configuration   = NetApp

Ready.
```

Enter the command:

storage bridge run-cli -name bridge_A1 -command "sasportlist"

```
SASPortList

;Connector      PHY     Link            Speed   SAS Address
;=============================================================
Device  A       1       Up              6Gb     5001086000a1c700
Device  A       2       Up              6Gb     5001086000a1c700
Device  A       3       Up              6Gb     5001086000a1c700
Device  A       4       Up              6Gb     5001086000a1c700
Device  B       1       Disabled        12Gb    5001086000a1c704
Device  B       2       Disabled        12Gb    5001086000a1c704
Device  B       3       Disabled        12Gb    5001086000a1c704
Device  B       4       Disabled        12Gb    5001086000a1c704
Device  C       1       Disabled        12Gb    5001086000a1c708
Device  C       2       Disabled        12Gb    5001086000a1c708
Device  C       3       Disabled        12Gb    5001086000a1c708
Device  C       4       Disabled        12Gb    5001086000a1c708
Device  D       1       Disabled        12Gb    5001086000a1c70c
Device  D       2       Disabled        12Gb    5001086000a1c70c
Device  D       3       Disabled        12Gb    5001086000a1c70c
Device  D       4       Disabled        12Gb    5001086000a1c70c
```

2. If the bridge is in a fabric-attached MetroCluster configuration, disable all of the switch ports that connect to the bridge FC port or ports.
3. From the ONTAP cluster prompt, remove the bridge undergoing maintenance from health monitoring:
   a. Remove the bridge:
      storage bridge remove -name *bridge-name*
   b. View the list of monitored bridges and confirm that the removed bridge is not present:
      storage bridge show
4. Properly ground yourself.
5. Power down the ATTO bridge.

If you are using a…	Then…
FibreBridge 7600N or 7500N bridge	Remove the power cables connected to the bridge.
FibreBridge 6500N bridge	Turn off the power switch of the bridge.

6. Disconnect the cables that are connected to the old bridge.

   You should make note of the port to which each cable was connected.
7. Remove the old bridge from the rack.
8. Install the new bridge into the rack.
9. Reconnect the power cord and, if configuring for IP access to the bridge, a shielded Ethernet cable.

   You must not reconnect the SAS or FC cables at this time.
10. Connect the bridge to a power source, and then turn it on.

    The bridge Ready LED might take up to 30 seconds to illuminate, indicating that the bridge has completed its power-on self test sequence.
11. 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.
12. 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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

    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.

13. Configure the bridge.

    If you retrieved the configuration information from the old bridge, use the information to configure the new bridge.

    Be sure to make note of the user name and password that you designate.

    The *ATTO FibreBridge Installation and Operation Manual* for your bridge model has the most current information on available commands and how to use them.

    > 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.

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

       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

         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`

       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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

14. 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.

       > ⓘ The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the switch to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

       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.

       > ⓘ The FCConnMode setting is not required when configuring a FibreBridge 7600N bridge.

       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`***

    d. If you are configuring a FibreBridge 7600N or 7500N bridge, disable the unused SAS ports: **`SASPortDisable`** ***`sas-port`***

       > ⓘ SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used. If only SAS port A is used, then SAS ports B, C, and D must be disabled.

15. Secure access to the bridge and save the bridge's configuration.
    a. From the controller prompt check the status of the bridges: **`storage bridge show`**

       The output shows which bridge is not secured.

    b. Check the status of the unsecured bridge's ports: **`info`**

       The output shows the status of Ethernet ports MP1 and MP2.

    c. If Ethernet port MP1 is enabled, run the following command: **`set EthernetPort mp1 disabled`**

> If Ethernet port MP2 is also enabled, repeat the previous substep for port MP2.

d. Save the bridge’s configuration.

   You must run the following commands:

   `SaveConfiguration`

   `FirmwareRestart`

   You are prompted to restart the bridge.

16. Update the FibreBridge firmware on each bridge.

    If the new bridge is the same type as the partner bridge upgrade to the same firmware as the partner bridge. If the new bridge is a different type to the partner bridge, upgrade to the latest firmware supported by the bridge and version of ONTAP. See the section "Updating firmware on a FibreBridge bridge" in the *MetroCluster Maintenance Guide*.

17. Reconnect the SAS and FC cables to the same ports on the new bridge.

    If the new bridge is a FibreBridge 7600N or 7500N, you must replace the cables connecting the bridge to the top or bottom of the shelf stack. The FibreBridge 6500N bridge used SAS cables; the FibreBridge 7600N and 7500N bridges require mini-SAS cables for these connections.

    > 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). For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the correct orientation of the SAS cable connector varies.

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

If you are using the…	Then…
ATTO ExpressNAV GUI	a. In a supported web browser, enter the IP address of the bridge in the browser box. You are brought to the ATTO FibreBridge homepage, which has a link. 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 appears with a menu to the left. c. Click **Advanced** in the menu. d. View the connected devices: **`sastargets`** e. Click **Submit**.
Serial port connection	View the connected devices: **`sastargets`**

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

If the text response truncated appears at the beginning of the output, you can use Telnet to connect to the bridge, and then view all of the output by using the sastargets command.

The following output shows that 10 disks are connected:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

19. Verify that the command output shows that the bridge is connected to all of the appropriate disks and disk shelves in the stack.

If the output is…	Then…

Correct	Repeat Step Replace a SLE FC to SAS Bridge for each remaining bridge.
Not correct	a. Check for loose SAS cables or correct the SAS cabling by repeating Step Replace a SLE FC to SAS Bridge. b. Repeat Step Replace a SLE FC to SAS Bridge.

20. If the bridge is in a fabric-attached MetroCluster configuration, reenable the FC switch port that you disabled at the beginning of this procedure.

    This should be the port that connects to the bridge.

21. From the system console of both controller modules, verify that all of the controller modules have access through the new bridge to the disk shelves (that is, that the system is cabled for Multipath HA):

    `run local sysconfig`

    > It might take up to a minute for the system to complete discovery.

    If the output does not indicate Multipath HA, you must correct the SAS and FC cabling because not all of the disk drives are accessible through the new bridge.

    The following output states that the system is cabled for Multipath HA:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

    > When the system is not cabled as Multipath HA, restarting a bridge might cause loss of access to the disk drives and result in a multi-disk panic.

22. If running ONTAP 9.4 or earlier, verify that the bridge is configured for SNMP.

    If you are using the bridge CLI, run the following command:

```
get snmp
```

23. From the ONTAP cluster prompt, add the bridge to health monitoring:

    a. Add the bridge, using the command for your version of ONTAP:

ONTAP version	Command
9.5 and later	**storage bridge add -address 0.0.0.0 -managed-by in-band -name *bridge-name***
9.4 and earlier	**storage bridge add -address *bridge-ip-address* -name *bridge-name***

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.

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

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status
Vendor Model                Bridge WWN
------------------  ------------- ------------  -------------
------ -----------------    ----------
ATTO_10.10.20.10  atto01        true          ok             Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok             Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok             Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok             Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

24. Verify the operation of the MetroCluster configuration in ONTAP:

a. Check whether the system is multipathed:
node run -node *node-name* sysconfig -a

b. Check for any health alerts on both clusters:
system health alert show

c. Confirm the MetroCluster configuration and that the operational mode is normal:
metrocluster show

d. Perform a MetroCluster check:
metrocluster check run

e. Display the results of the MetroCluster check:
   `metrocluster check show`
f. Check for any health alerts on the switches (if present):
   `storage switch show`
g. Run Config Advisor.

   NetApp Downloads: Config Advisor

h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Related information

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

Hot-swapping a FibreBridge 7500N with a 7600N bridge

You can hot-swap a FibreBridge 7500N bridge with a 7600N bridge.

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.

> Starting with ONTAP 9.8, the **`storage bridge`** command is replaced with **`system bridge`**. The following steps show the **`storage bridge`** command, but if you are running ONTAP 9.8 or later, the **`system bridge`** command is preferred.

Steps

1. If the bridge is in a fabric-attached MetroCluster configuration, disable all of the switch ports that connect to the bridge FC port or ports.
2. From the ONTAP cluster prompt, remove the bridge undergoing maintenance from health monitoring:
   a. Remove the bridge:
      `storage bridge remove -name` ***`bridge-name`***
   b. View the list of monitored bridges and confirm that the removed bridge is not present:
      `storage bridge show`
3. Properly ground yourself.
4. Remove the power cables connected to the bridge to power down the bridge.
5. Disconnect the cables that are connected to the old bridge.

   You should make note of the port to which each cable was connected.

6. Remove the old bridge from the rack.
7. Install the new bridge into the rack.
8. Reconnect the power cord and shielded Ethernet cable.

   > You must not reconnect the SAS or FC cables at this time.

9. Connect the bridge to a power source, and then turn it on.

The bridge Ready LED might take up to 30 seconds to illuminate, indicating that the bridge has completed its power-on self test sequence.

10. 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.

11. 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.

12. 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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

    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.

13. Configure the bridges.

    Be sure to make note of the user name and password that you designate.

    The *ATTO FibreBridge Installation and Operation Manual* for your bridge model has the most current information on available commands and how to use them.

    > Do not configure time synchronization on FibreBridge 7600N. The time synchronization for FibreBridge 7600N 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.

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

       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

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`

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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

14. 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.

> ⓘ 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.

If using the CLI, you must run the following command: **`set FCDataRate`** ***`port-number port-speed`***

a. 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 unused port: + **`FCPortDisable port-number`** The following example shows the disabling of FC port 2:

```
`FCPortDisable 2`

Fibre Channel Port 2 has been disabled.
```

b. Disable the unused SAS ports:
SASPortDisable *sas-port*

> SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used.

If only SAS port A is used, then SAS ports B, C, and D must be disabled. The following example shows disabling of SAS port B. You must similarly disable SAS ports C and D:

```
`SASPortDisable b`

SAS Port B has been disabled.
```

15. Secure access to the bridge and save the bridge's configuration.
    a. From the controller prompt check the status of the bridges: **storage bridge show**

       The output shows which bridge is not secured.

    b. Check the status of the unsecured bridge's ports: **info**

       The output shows the status of Ethernet ports MP1 and MP2.

    c. If Ethernet port MP1 is enabled, run the following command:
       set EthernetPort mp1 disabled

       > If Ethernet port MP2 is also enabled, repeat the previous substep for port MP2.

    d. Save the bridge's configuration.

       You must run the following commands:

       SaveConfiguration

       FirmwareRestart

       You are prompted to restart the bridge.

16. Update the FibreBridge firmware on each bridge.

    Updating firmware on FibreBridge 7600N or 7500N bridges on configurations running ONTAP 9.4 and later

17. Reconnect the SAS and FC cables to the same ports on the new bridge.

> 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). For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the correct orientation of the SAS cable connector varies.

18. Verify that each bridge can see all of the disk drives and disk shelves to which the bridge is connected:

sastargets

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

The following output shows that 10 disks are connected:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

19. Verify that the command output shows that the bridge is connected to all of the appropriate disks and disk shelves in the stack.

If the output is…	Then…
Correct	Repeat the previous step for each remaining bridge.
Not correct	a. Check for loose SAS cables or correct the SAS cabling by repeating Step task_replace_a_sle_fc_to_sas_bridge.md#STEP_CD84065D8F3B43F192919B0CD6FDC1A6. b. Repeat the previous step.

20. If the bridge is in a fabric-attached MetroCluster configuration, reenable the FC switch port that you disabled at the beginning of this procedure.

    This should be the port that connects to the bridge.

21. From the system console of both controller modules, verify that all of the controller modules have access through the new bridge to the disk shelves (that is, that the system is cabled for Multipath HA):

    run local sysconfig

    It might take up to a minute for the system to complete discovery.

    If the output does not indicate Multipath HA, you must correct the SAS and FC cabling because not all of the disk drives are accessible through the new bridge.

The following output states that the system is cabled for Multipath HA:

```
NetApp Release 8.3.2: Tue Jan 26 01:41:49 PDT 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

> When the system is not cabled as Multipath HA, restarting a bridge might cause loss of access to the disk drives and result in a multi-disk panic.

22. If running ONTAP 9.4 or earlier, verify that the bridge is configured for SNMP.

    If you are using the bridge CLI, run the following command:

```
get snmp
```

23. From the ONTAP cluster prompt, add the bridge to health monitoring:

    a. Add the bridge, using the command for your version of ONTAP:

ONTAP version	Command
9.5 and later	**`storage bridge add -address 0.0.0.0 -managed-by in-band -name`** ***`bridge-name`***
9.4 and earlier	**`storage bridge add -address`** ***`bridge-ip-address`*** **`-name`** ***`bridge-name`***

    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.

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

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status
Vendor Model                Bridge WWN
------------------  ------------- ------------  --------------
------ -----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

24. Verify the operation of the MetroCluster configuration in ONTAP:
    a. Check whether the system is multipathed:
       node run -node *node-name* sysconfig -a
    b. Check for any health alerts on both clusters:
       system health alert show
    c. Confirm the MetroCluster configuration and that the operational mode is normal:
       metrocluster show
    d. Perform a MetroCluster check:
       metrocluster check run
    e. Display the results of the MetroCluster check:

       metrocluster check show

    f. Check for any health alerts on the switches (if present):
       storage switch show
    g. Run Config Advisor.

       NetApp Downloads: Config Advisor

    h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Related information

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

Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge

You can hot-swap a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge to replace a failed bridge or upgrade your bridge in a fabric-attached or a bridge-attached MetroCluster configuration.

- This procedure is for hot-swapping a single FibreBridge 6500N bridge with single FibreBridge 7600N or 7500N bridge.
- When you hot-swap a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge, you must use only one FC port and one SAS port on the FibreBridge 7600N or 7500N bridge.
- 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.

> ⓘ If you are hot-swapping both FibreBridge 6500N bridges in a pair, you must use the Consolidate Multiple Storage Stacks procedure for zoning instructions. By replacing both FibreBridge 6500N bridges on the bridge, you can take advantage of the additional ports on the FibreBridge 7600N or 7500N bridge.

> ⓘ Starting with ONTAP 9.8, the **`storage bridge`** command is replaced with **`system bridge`**. The following steps show the **`storage bridge`** command, but if you are running ONTAP 9.8 or later, the **`system bridge`** command is preferred.

Steps

1. Do one of the following:
   - If the failed bridge is in a fabric-attached MetroCluster configuration, disable the switch port that connects to the bridge FC port.
   - If the failed bridge is in a stretch MetroCluster configuration, use either one of the available FC ports.
2. From the ONTAP cluster prompt, remove the bridge undergoing maintenance from health monitoring:
   a. Remove the bridge:
      `storage bridge remove -name` ***`bridge-name`***
   b. View the list of monitored bridges and confirm that the removed bridge is not present:
      `storage bridge show`
3. Properly ground yourself.
4. Turn off the power switch of the bridge.
5. Disconnect the cables connected from the shelf to the FibreBridge 6500N bridge ports and power cables.

   You should make note of the ports that each cable was connected to.

6. Remove the FibreBridge 6500N bridge that you need to replace from the rack.
7. Install the new FibreBridge 7600N or 7500N bridge into the rack.
8. Reconnect the power cord and, if necessary, the shielded Ethernet cable.

   > ⓘ Do not reconnect the SAS or FC cables at this time.

9. 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.

10. 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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

    The Ethernet management 1 port enables you to quickly download the bridge firmware (using ATTO ExpressNAV or FTP management interfaces) and to retrieve core files and extract logs.

11. 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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

    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.

12. Configure the bridge.

    If you retrieved the configuration information from the old bridge, use the information to configure the new bridge.

    Be sure to make note of the user name and password that you designate.

    The *ATTO FibreBridge Installation and Operation Manual* for your bridge model has the most current information on available commands and how to use them.

    > 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.

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

       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

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

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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

13. 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.

> The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the switch to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

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.

> The FCConnMode setting is not required when configuring a FibreBridge 7600N bridge.

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`***

d. If you are configuring a FibreBridge 7600N or 7500N bridge, disable the unused SAS ports:
`SASPortDisable` ***`sas-port`***

> SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used. If only SAS port A is used, then SAS ports B, C, and D must be disabled.

14. Secure access to the bridge and save the bridge's configuration.

a. From the controller prompt check the status of the bridges:
`storage bridge show`

The output shows which bridge is not secured.

b. Check the status of the unsecured bridge's ports: **`info`**

The output shows the status of Ethernet ports MP1 and MP2.

c. If Ethernet port MP1 is enabled, run the following command:
`set EthernetPort mp1 disabled`

> If Ethernet port MP2 is also enabled, repeat the previous substep for port MP2.

d. Save the bridge's configuration.

You must run the following commands:

`SaveConfiguration`

`FirmwareRestart`

You are prompted to restart the bridge.

15. Turn on Health Monitoring for the FibreBridge 7600N or 7500N bridge.
16. Update the FibreBridge firmware on each bridge.

If the new bridge is the same type as the partner bridge upgrade to the same firmware as the partner bridge. If the new bridge is a different type to the partner bridge, upgrade to the latest firmware supported by the bridge and version of ONTAP. See the section "Updating firmware on a FibreBridge bridge" in the *MetroCluster Maintenance Guide*.

17. Reconnect the SAS and FC cables to the SAS A and Fibre Channel 1 ports on the new bridge.

The SAS port must be cabled to the same shelf port that the FibreBridge 6500N bridge had been connected to.

The FC port must be cabled to the same switch or controller port that the FibreBridge 6500N bridge had been connected to.

Do not force a connector into a port. The mini-SAS cables are keyed; when oriented correctly into a SAS port, the SAS cable 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).For controllers, the orientation of SAS ports can vary depending on the platform model; therefore, the correct orientation of the SAS cable connector varies.

18. Verify that the bridge can see all of the disk drives and disk shelves it is connected to.

If you are using the…	Then…
ATTO ExpressNAV GUI	a. In a supported web browser, enter the IP address of the bridge in the browser box. You are brought to the ATTO FibreBridge homepage, which has a link. 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 appears with a menu to the left. c. Click **Advanced** in the menu. d. Enter the following command and then click **Submit** to see the list of disks visible to the bridge: **`sastargets`**
Serial port connection	Display the list of disks visible to the bridge: **`sastargets`**

The 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. For example, the following output shows that 10 disks are connected:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

If the text `response truncated` appears at the beginning of the output, you can use Telnet to access the bridge and enter the same command to see all of the output.

19. Verify that the command output shows that the bridge is connected to all of the necessary disks and disk shelves in the stack.

If the output is…	Then…
Correct	Repeat Step Replace a SLE FC to SAS Bridge for each remaining bridge.]
Not correct	a. Check for loose SAS cables or correct the SAS cabling by repeating Step task_replace_a_sle_fc_to_sas_bridge.md#STEP_CD84065D8F3B43F192919B0CD6FDC1A6. b. Repeat Step Replace a SLE FC to SAS Bridge for each remaining bridge.].

20. Reenable the FC switch port that connects to the bridge.
21. Verify that all controllers have access through the new bridge to the disk shelves (that the system is cabled for Multipath HA), at the system console of both controllers: `run local sysconfig`

    It might take up to a minute for the system to complete discovery.

    For example, the following output shows that the system is cabled for Multipath HA:

```
NetApp Release 8.3.2: Tue Jan 26 01:23:24 PST 2016
System ID: 1231231231 (node_A_1); partner ID: 4564564564 (node_A_2)
System Serial Number: 700000123123 (node_A_1); partner Serial Number:
700000456456 (node_A_2)
System Rev: B0
System Storage Configuration: Multi-Path HA
System ACP Connectivity: NA
```

    If the command output indicates that the configuration is mixed-path or single-path HA, you must correct the SAS and FC cabling because not all disk drives are accessible through the new bridge.

    When the system is not cabled as Multipath HA, restarting a bridge might cause loss of access to the disk drives and result in a multi-disk panic.

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

ONTAP version	Command

9.5 and later	**storage bridge add -address 0.0.0.0 -managed-by in-band -name *bridge-name***
9.4 and earlier	**storage bridge add -address *bridge-ip-address* -name *bridge-name***

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.

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

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status
Vendor Model                Bridge WWN
------------------  ------------- ------------  -------------
------ -----------------    ----------
ATTO_10.10.20.10  atto01        true          ok             Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok             Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok             Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok             Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

23. Verify the operation of the MetroCluster configuration in ONTAP:

a. Check whether the system is multipathed:

node run -node *node-name* sysconfig -a

b. Check for any health alerts on both clusters:
system health alert show

c. Confirm the MetroCluster configuration and that the operational mode is normal:

metrocluster show

d. Perform a MetroCluster check:

```
metrocluster check run
```

e. Display the results of the MetroCluster check:

```
metrocluster check show
```

f. Check for any health alerts on the switches (if present):

```
storage switch show
```

g. Run Config Advisor.

NetApp Downloads: Config Advisor

h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

24. Return the failed part to NetApp as described in the RMA instructions shipped with the kit.

    Contact technical support at NetApp Support, 888-463-8277 (North America), 00-800-44-638277 (Europe), or +800-800-80-800 (Asia/Pacific) if you need the RMA number or additional help with the replacement procedure.

Related information

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

Replacing a pair of FibreBridge 6500N bridges with 7600N or 7500N bridges

To take advantage of the additional FC2 port on the FibreBridge 7600N or 7500N bridges and reduce rack utilization, you can nondisruptively replace 6500N bridges and consolidate up to four storage stacks behind a single pair of FibreBridge 7600N or 7500N bridges.

You need the admin password and access to an FTP or SCP server.

You should use this procedure if:

- You are replacing a pair of FibreBridge 6500N bridges with FibreBridge 7600N or 7500N bridges.

  After the replacement, both bridges in the pair must be the same model.

- You previously replaced a single FibreBridge 6500N bridge with a 7600N or 7500N bridge and are now replacing the second bridge in the pair.
- You have a pair of FibreBridge 7600N or 7500N bridges with available SAS ports and you are consolidating SAS storage stacks that are currently connected using FibreBridge 6500N bridges.

This procedure is nondisruptive and takes approximately two hours to complete.

Related information

Replacing a single FC-to-SAS bridge

Verifying storage connectivity

Before replacing bridges, you should verify bridge and storage connectivity. Familiarizing yourself with the command output enables you to subsequently confirm connectivity after making configuration changes.

You can issue these commands from the admin prompt of any of the controller modules in the MetroCluster configuration at the site undergoing maintenance.

1. Confirm connectivity to the disks by entering the following command on any one of the MetroCluster nodes:

   `run local sysconfig -v`

   The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
```

```
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Hot-swapping FibreBridge 6500N bridges to create a pair of FibreBridge 7600N or 7500N bridges

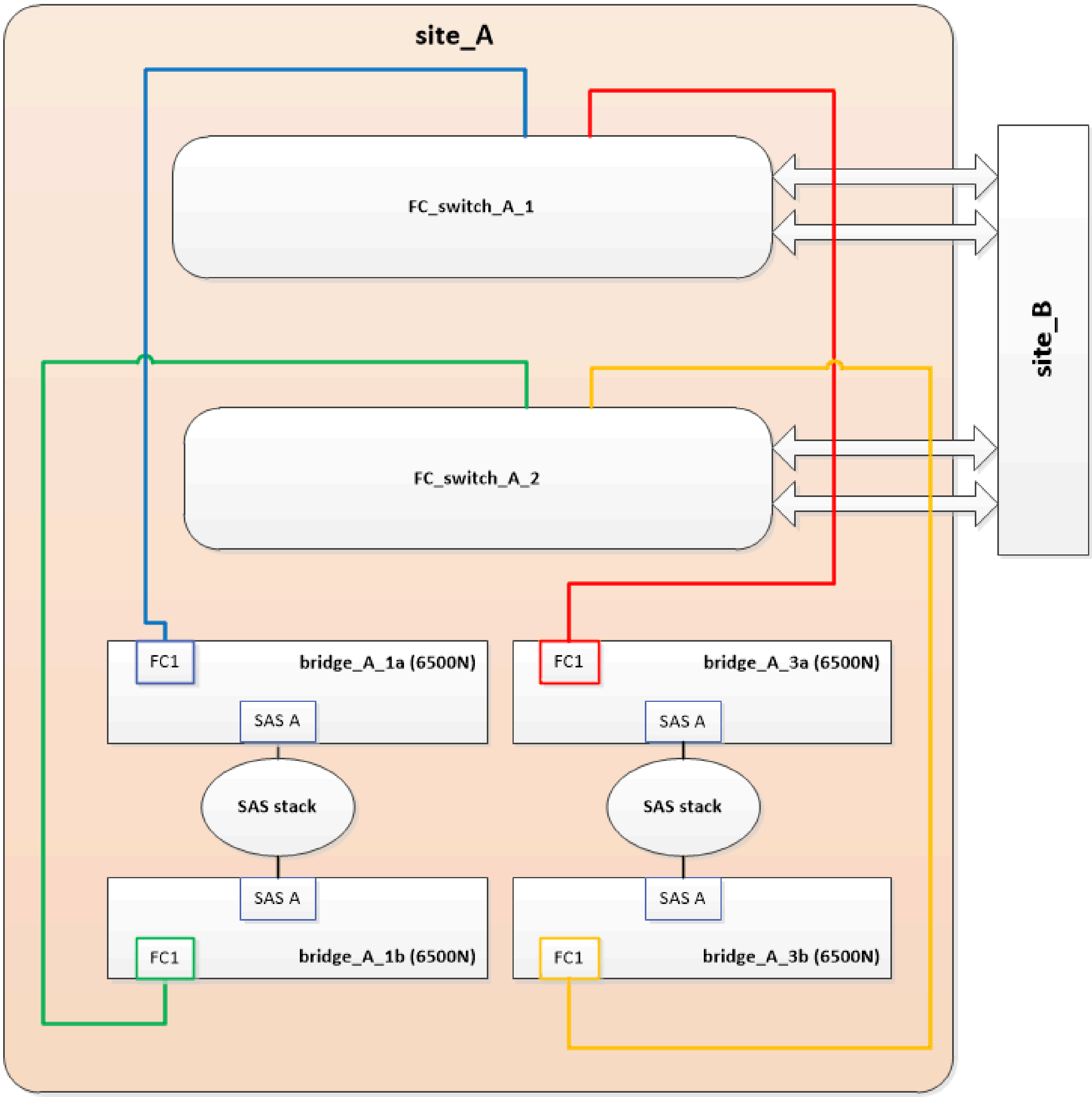
To hot-swap one or two FibreBridge 6500N bridges to create a configuration with a pair of FibreBridge 7600N or 7500N bridges, you must replace the bridges one at a time and follow the correct cabling procedure. The new cabling is different from the original cabling.

You can also use this procedure if the following conditions are true:

- You are replacing a pair of FibreBridge 6500N bridges that are both connected to the same stack of SAS storage.
- You previously replaced one FibreBridge 6500N bridge in the pair, and your storage stack is configured with one FibreBridge 6500N bridge and one FibreBridge 7600N or 7500N bridge.

  In this case, you should start with the step below to hot-swap the “bottom” FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge.

The following diagram shows an example of the initial configuration, in which four FibreBridge 6500N bridges are connecting two SAS storage stacks:



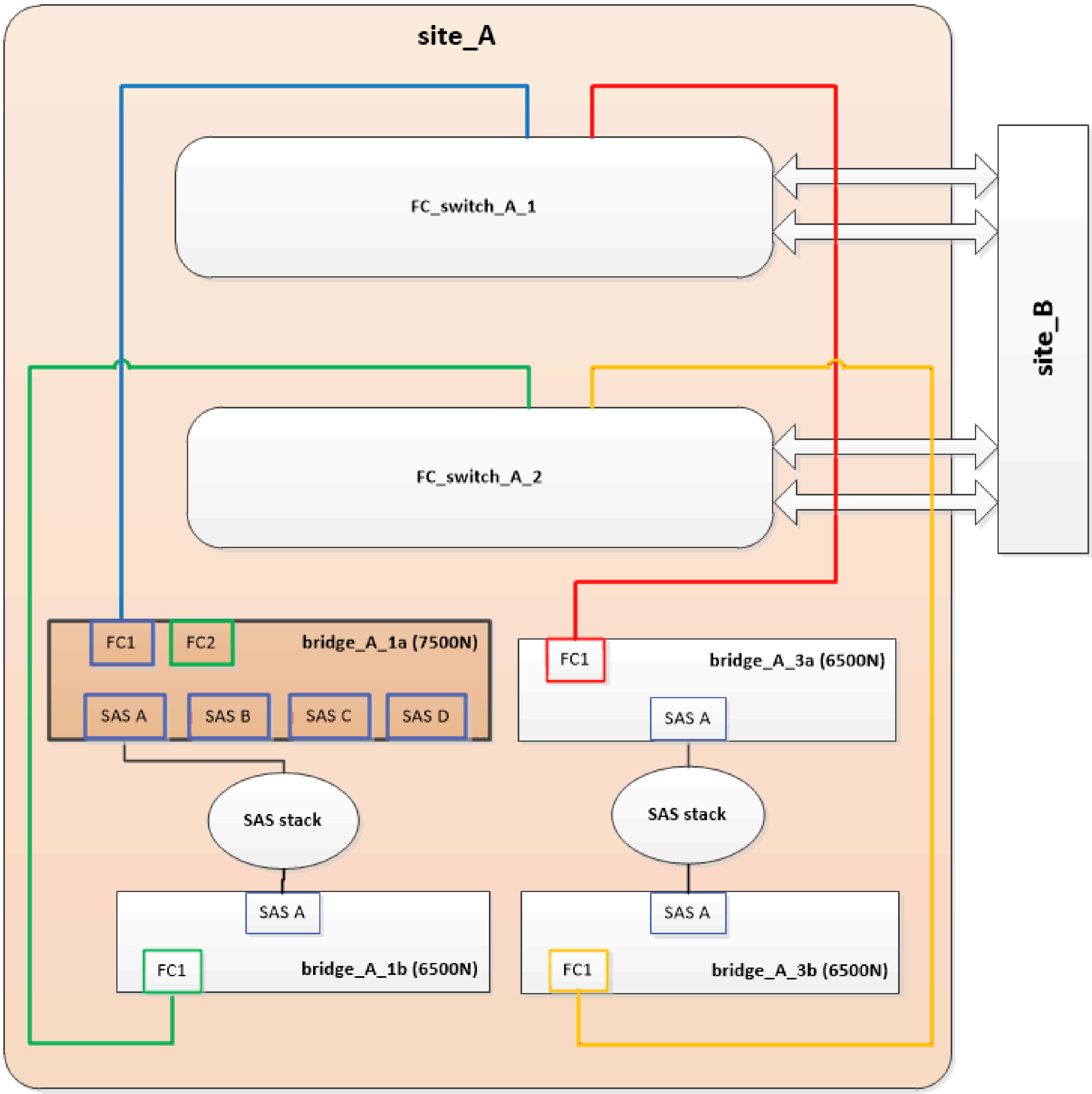
Steps

1. Using the following guidelines, hot-swap the "`top`"FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge using the procedure in Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge:

    - Connect the FibreBridge 7600N or 7500N bridge FC1 port to the switch or controller.

      This is the same connection that was made to the FibreBridge 6500N bridge FC1 port.

    - Do not connect the FibreBridge 7600N or 7500N bridge FC2 port at this time. The following diagram shows that bridge_A_1a has been replaced and is now a FibreBridge 7600N or 7500N bridge:



2. Confirm connectivity to the bridge-connected disks and that the new FibreBridge 7500N is visible in the configuration:

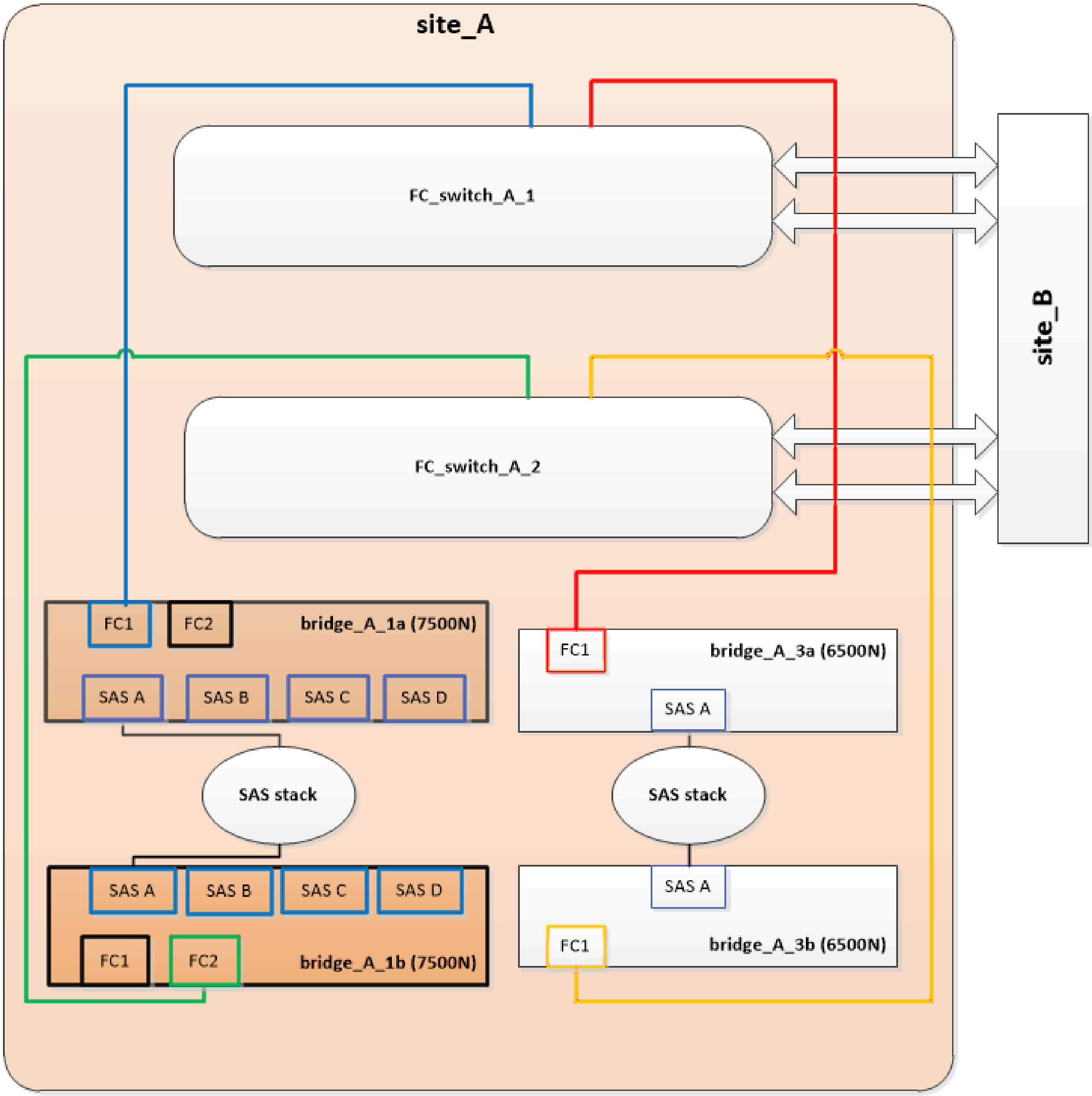
run local sysconfig -v

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
```

```
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104**<===**
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

3. Using the following guidelines, hot-swap the "`bottom`"FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge using the procedure in Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge:
   - Connect the FibreBridge 7600N or 7500N bridge FC2 port to the switch or controller.

     This is the same connection that was made to the FibreBridge 6500N bridge FC1 port.
   - Do not connect the FibreBridge 7600N or 7500N bridge FC1 port at this time.



4. Confirm connectivity to the bridge-connected disks:

   `run local sysconfig -v`

   The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
```

```
.
.
.
```

Cabling the bridge SAS ports when consolidating storage behind FibreBridge 7600N or 7500N bridges

When consolidating multiple SAS storage stacks behind a single pair of FibreBridge 7600N or 7500N bridges with available SAS ports, you must move the top and bottom SAS cables to the new bridges.

The FibreBridge 6500N bridge SAS ports use QSFP connectors. The FibreBridge 7600N or 7500N bridge SAS ports use mini-SAS connectors.

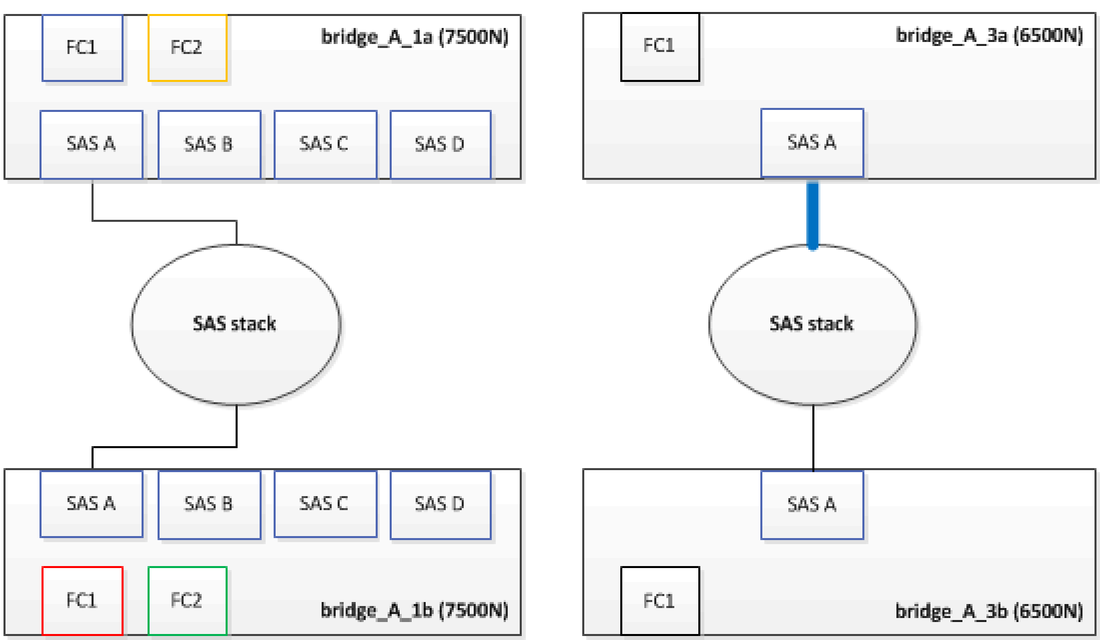
> If you insert a SAS cable into the wrong port, when you remove the cable from a SAS port, you must wait at least 120 seconds before plugging the cable into a different SAS port. If you fail to do so, the system will not recognize that the cable has been moved to another port.

> 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).

Steps

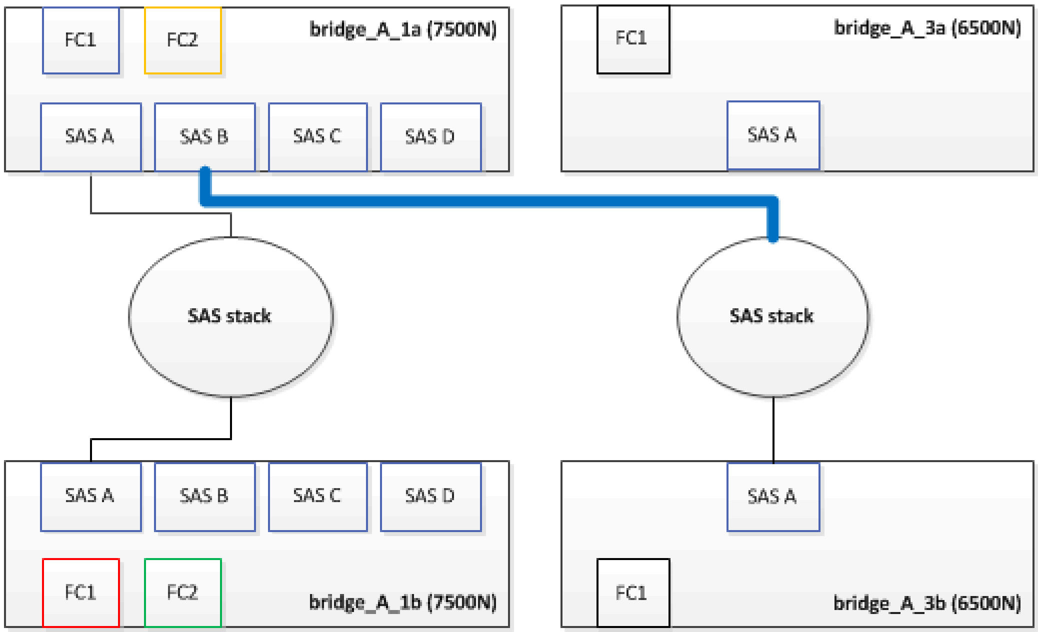
1. Remove the cable that connects the SAS A port of the top FibreBridge 6500N bridge to the top SAS shelf, being sure to note the SAS port on the storage shelf to which it connects.

   The cable is shown in blue in the following example:



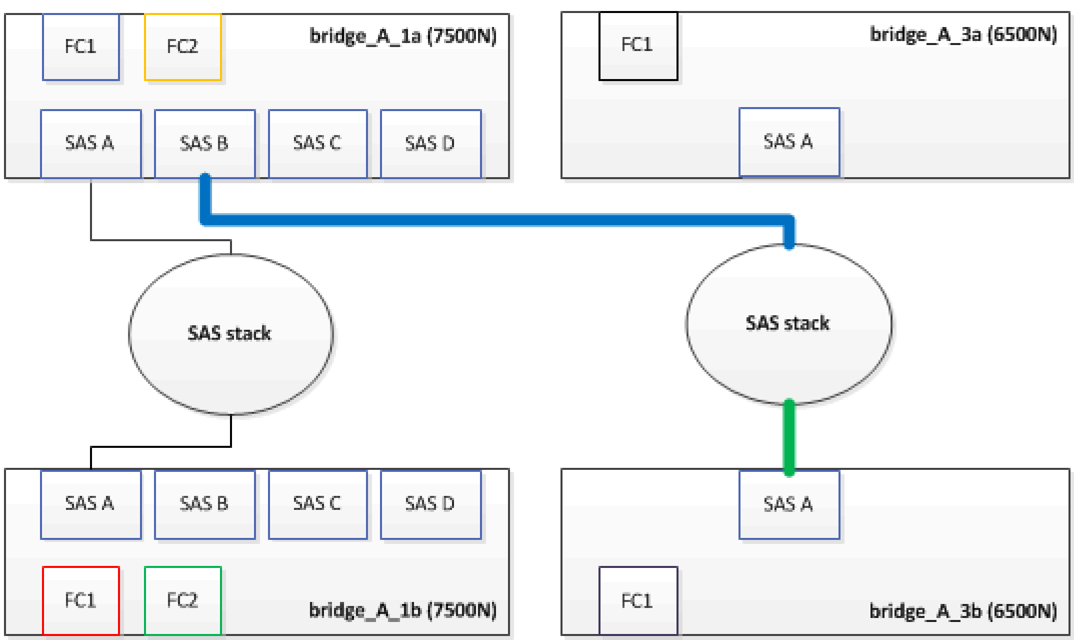
2. Using a cable with a mini-SAS connector, connect the same SAS port on the storage shelf to the SAS B port of the top FibreBridge 7600N or 7500N bridge.

   The cable is shown in blue in the following example:



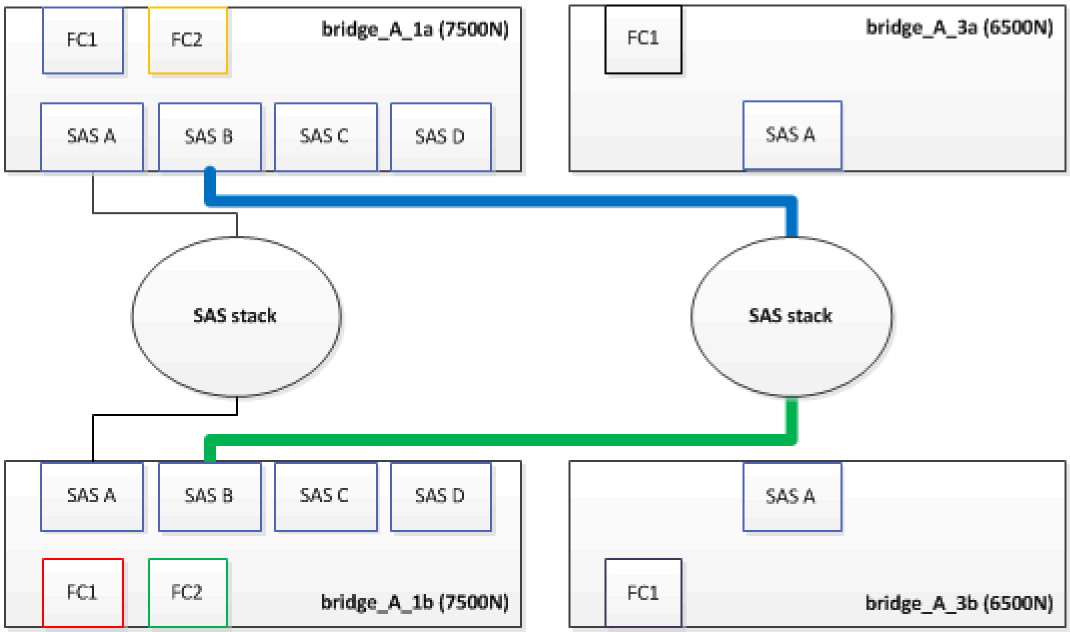
3. Remove the cable that connects the SAS A port of the bottom FibreBridge 6500N bridge to the top SAS shelf, being sure to note the SAS port on the storage shelf to which it connects.

   This cable is shown in green in the following example:



4. Using a cable with a mini-SAS connector, connect the same SAS port on the storage shelf to the SAS B port of the bottom FibreBridge 7600N or 7500N bridge.

   This cable is shown in green in the following example:



5. Confirm connectivity to the bridge-connected disks:

   `run local sysconfig -v`

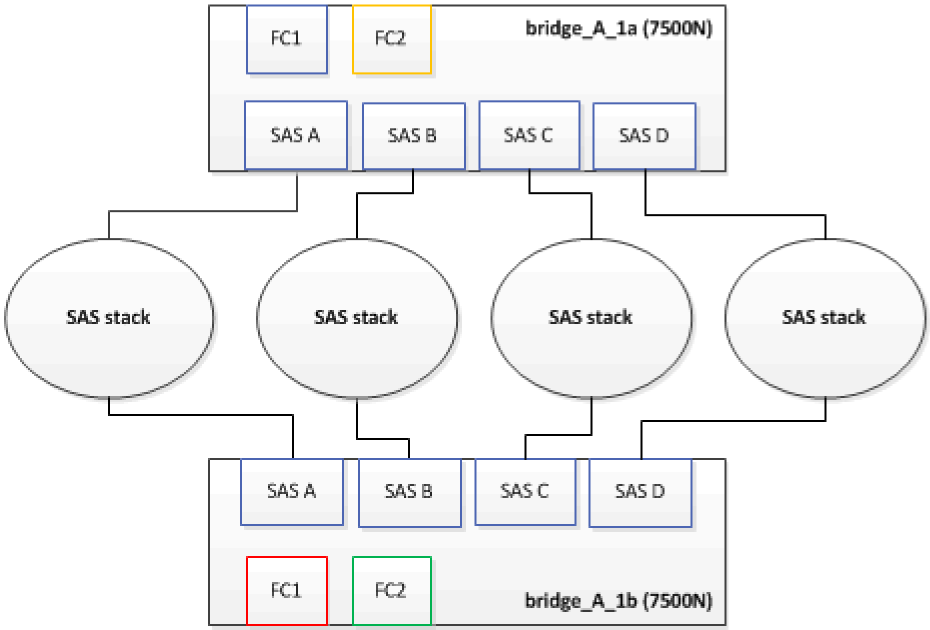
   The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
```

```
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

6. Remove the old FibreBridge 6500N bridges that are no longer connected to the SAS storage.
7. Wait two minutes for the system to recognize the changes.
8. If the system was miscabled, remove the cable, correct the cabling, and then reconnect the correct cable.
9. If necessary, repeat the preceding steps to move up to two additional SAS stacks behind the new FibreBridge 7600N or 7500N bridges, using SAS ports C and then D.

   Each SAS stack must be connected to the same SAS port on the top and bottom bridge. For example, if the top connection of the stack is connected to the top bridge SAS B port, the bottom connection must be connected to the SAS B port of the bottom bridge.



Updating zoning when adding FibreBridge 7600N or 7500N bridges to a configuration

The zoning must be changed when you are replacing FibreBridge 6500N bridges with FibreBridge 7600N or 7500N bridges and using both FC ports on the FibreBridge 7600N or 7500N bridges. The required changes depend on whether you are running a version of ONTAP earlier than 9.1 or 9.1 and later.

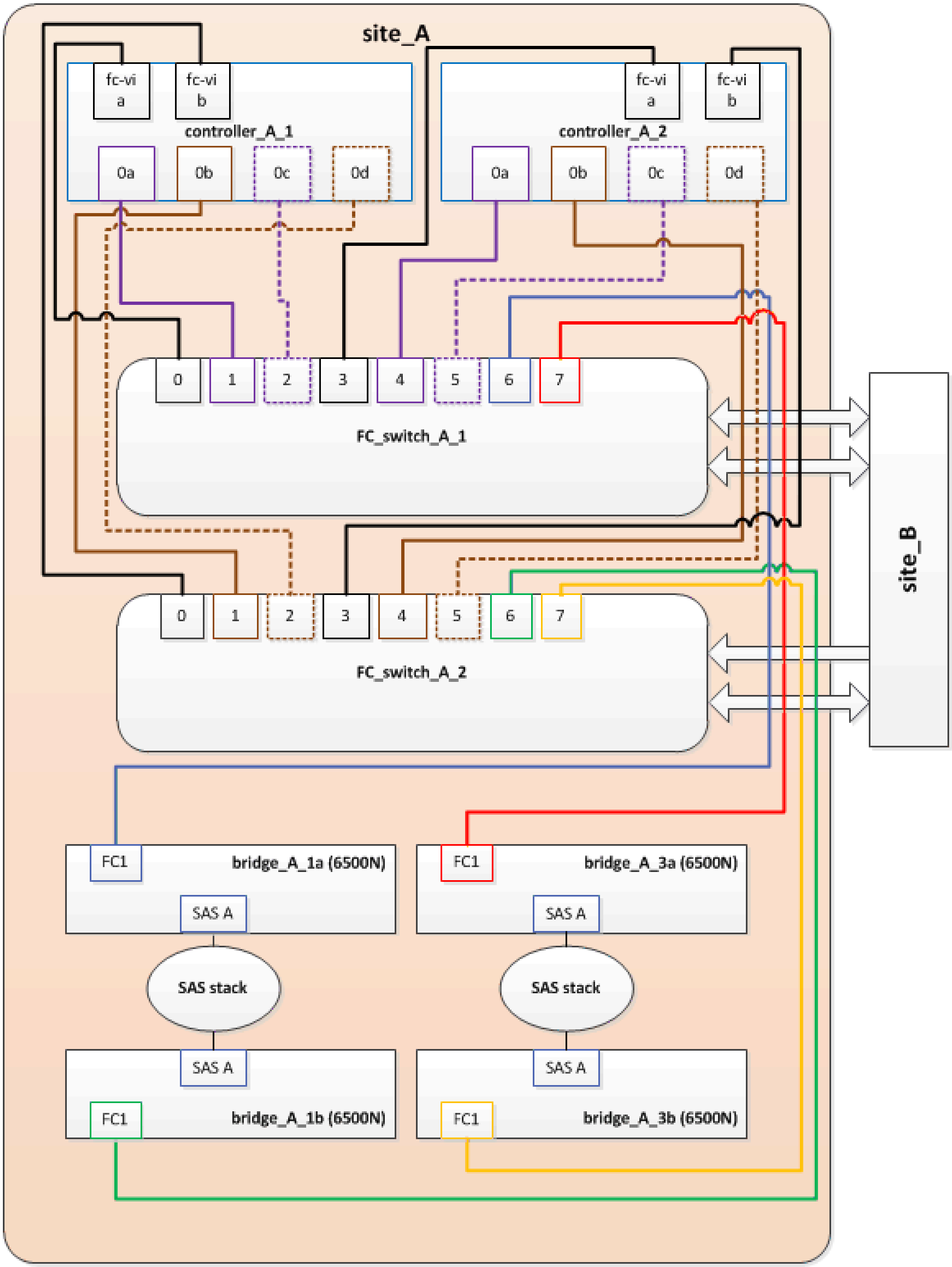
Updating zoning when adding FibreBridge 7500N bridges to a configuration (prior to ONTAP 9.1)

The zoning must be changed when you are replacing FibreBridge 6500N bridges with FibreBridge 7500N bridges and using both FC ports on the FibreBridge 7500N bridges. Each zone can have no more than four initiator ports. The zoning you use depends on whether you are running ONTAP prior to version 9.1 or 9.1 and later

The specific zoning in this task is for versions of ONTAP prior to version 9.1.

The zoning changes are required to avoid issues with ONTAP, which requires that no more than four FC initiator ports can have a path to a disk. After recabling to consolidate the shelves, the existing zoning would result in each disk being reachable by eight FC ports. You must change the zoning to reduce the initiator ports in each zone to four.

The following diagram shows the zoning on site_A before the changes:



Steps

1. Update the storage zones for the FC switches by removing half of the initiator ports from each existing zone and creating new zones for the FibreBridge 7500N FC2 ports.

   The zones for the new FC2 ports will contain the initiator ports removed from the existing zones. In the diagrams, these zones are shown with dashed lines.

   For details about the zoning commands, see the FC switch sections of the Fabric-attached MetroCluster installation and configuration or Stretch MetroCluster installation and configuration.

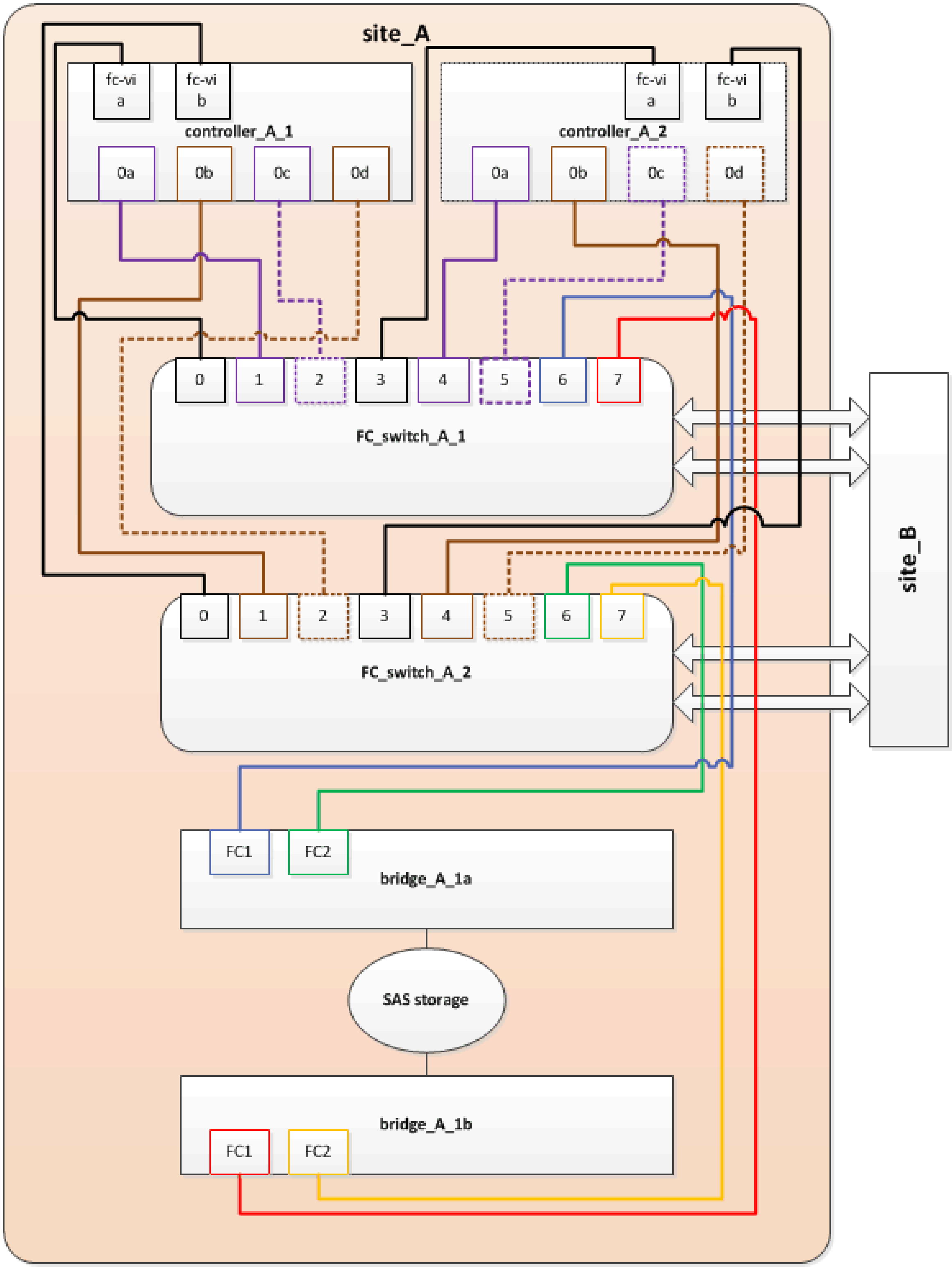
The following examples show the storage zones and the ports in each zone before and after the consolidation. The ports are identified by *domain, port* pairs.

- Domain 5 consists of switch FC_switch_A_1.
- Domain 6 consists of switch FC_switch_A_2.
- Domain 7 consists of switch FC_switch_B_1.
- Domain 8 consists of switch FC_switch_B_2.

Before or after consolidation	Zone	Domains and ports	Colors in diagram*
Zones before the consolidation. There is a zone for each FC port on the four FibreBridge 6500N bridges.	STOR_A_1a-FC1	5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,6	Purple + dashed purple + blue
	STOR_A_1b-FC1	6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,6	Brown + dashed brown + green
	STOR_A_2a-FC1	5,1; 5,2; 5,4; 5,5; 7,1; 7,2; 7,4; 7,5; 5,7	Purple + dashed purple + red
	STOR_A_2b-FC1	6,1; 6,2; 6,4; 6,5; 8,1; 8,2; 8,4; 8,5; 6,7	Brown + dashed brown + orange
Zones after the consolidation. There is a zone for each FC port on the two FibreBridge 7500N bridges.	STOR_A_1a-FC1	7,1; 7,4; 5,1; 5,4; 5,6	Purple + blue
	STOR_A_1b-FC1	7,2; 7,5; 5,2; 5,5; 5,7	Dashed purple + red
	STOR_A_1a-FC2	8,1; 8,4; 6,1; 6,4; 6,6	Brown + green
	STOR_A_1b-FC2	8,2; 8,5; 6,2; 6,5; 6,7	Dashed brown + orange

- The diagrams only show site_A.

  The following diagram shows zoning at site_A after the consolidation:



Updating zoning when adding FibreBridge 7600N or 7500N bridges to a configuration (ONTAP 9.1 and later)

The zoning must be changed when you are replacing FibreBridge 6500N bridges with FibreBridge 7600N or 7500N bridges and using both FC ports on the FibreBridge 7600N or 7500N bridges. Each zone can have no more than four initiator ports.

- This task applies to ONTAP 9.1 and later.

- FibreBridge 7600N bridges are supported in ONTAP 9.6 and later.
- The specific zoning in this task is for ONTAP 9.1 and later.
- The zoning changes are required to avoid issues with ONTAP, which requires that no more than four FC initiator ports can have a path to a disk.

  After recabling to consolidate the shelves, the existing zoning would result in each disk being reachable by eight FC ports. You must change the zoning to reduce the initiator ports in each zone to four.

  1. Update the storage zones for the FC switches by removing half of the initiator ports from each existing zone and creating new zones for the FibreBridge 7600N or 7500N FC2 ports.

     The zones for the new FC2 ports will contain the initiator ports removed from the existing zones.

     The FC switch section of the *Fabric-attached MetroCluster Installation and Configuration Guide* contains details about the zoning commands.

     Fabric-attached MetroCluster installation and configuration

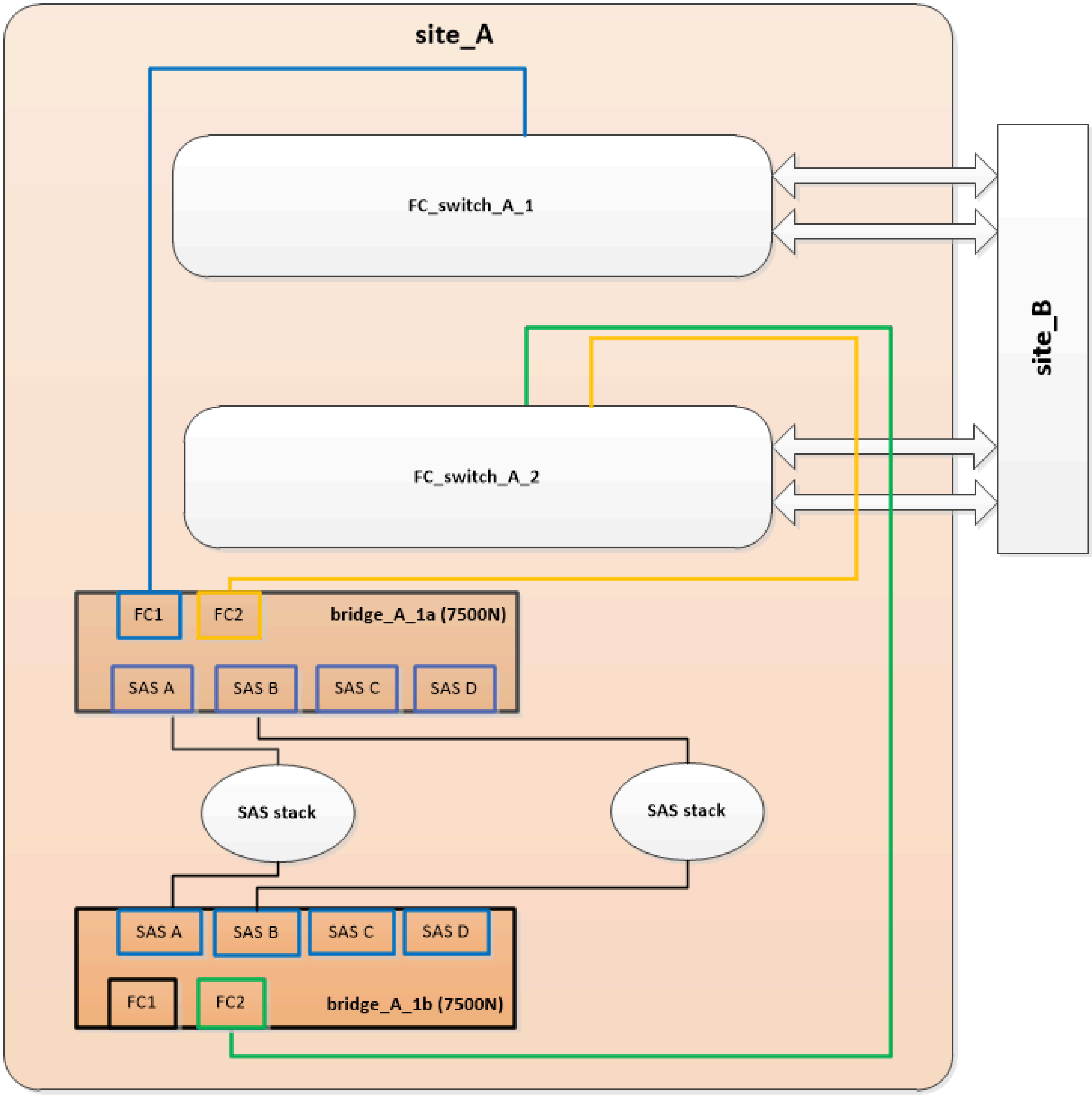
Cabling the second bridge FC port when adding FibreBridge 7600N or 7500N bridges to a configuration

To provide multiple paths to the storage stacks, you can cable the second FC port on each FibreBridge 7600N or 7500N bridge when you have added the FibreBridge 7600N or 7500N bridge to your configuration.

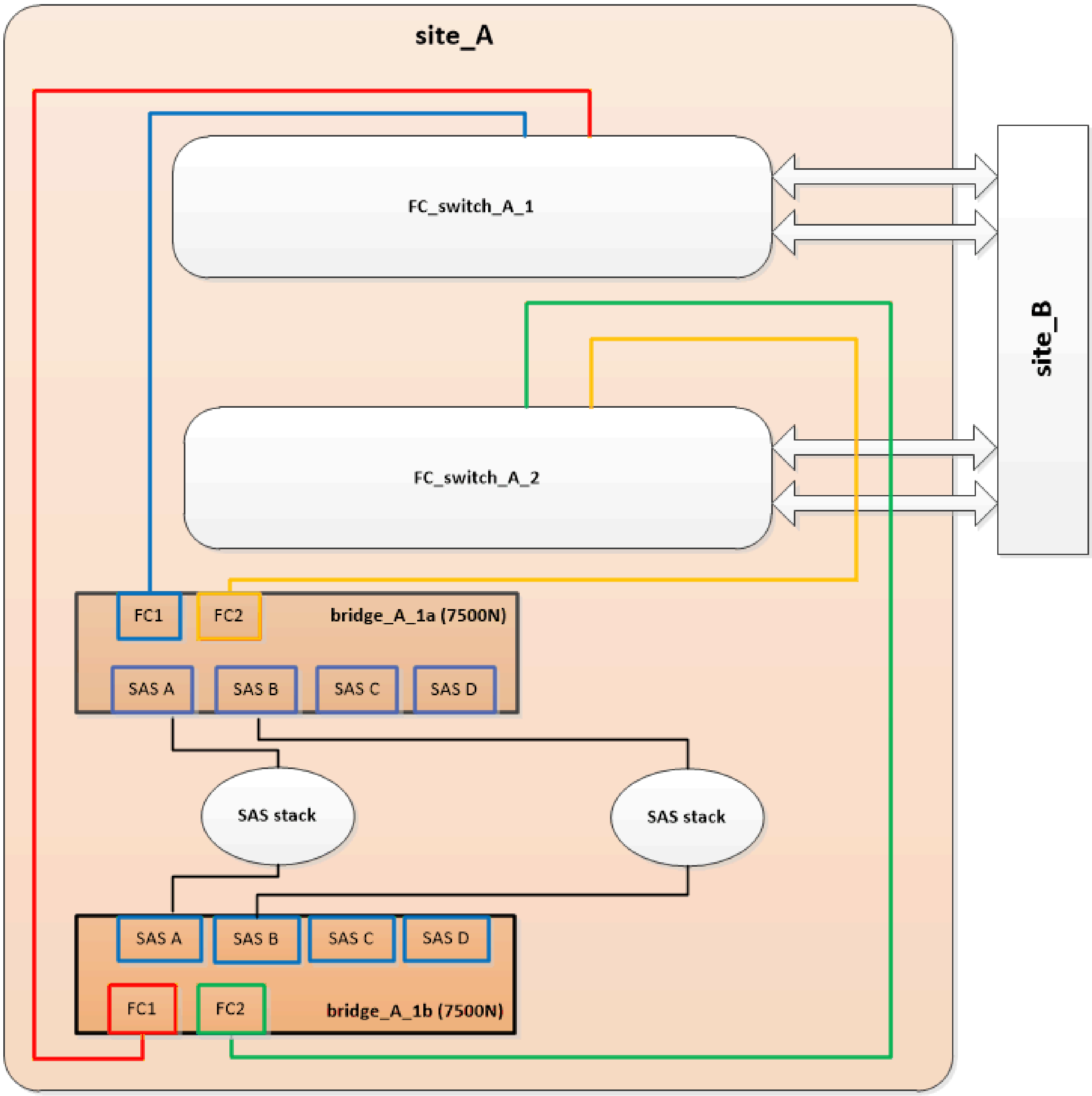
The zoning must have been adjusted to provide zones for the second FC ports.

Steps

1. Cable the FC2 port of the top bridge to the correct port on FC_switch_A_2.



2. Cable the FC1 port of the bottom bridge to the correct port on FC_switch_A_1.



3. Confirm connectivity to the bridge-connected disks:

   `run local sysconfig -v`

   The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2015
System ID: 0536872165 (node_A_1); partner ID: 0536872141 (node_B_1)
System Serial Number: 940001025465 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
```

```
be multi-path HA**
.
.
.
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60100
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        FINISAR CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0R1R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs40:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs40:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge7500N A30H
FB7500N100104
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

Disabling unused SAS ports on the FC-to-SAS bridges

After making cabling changes to the bridge, you should disable any unused SAS ports on FC-to-SAS bridges to avoid health monitor alerts related to the unused ports.

Steps

1. Disable unused SAS ports on the top FC-to-SAS bridge:
   a. Log in to the bridge CLI.
   b. Disable any unused ports.

   > ⓘ If you have configured an ATTO 7500N bridge, then all of the SAS ports (A through D) are enabled by default, and you must disable the SAS ports that are not being used:
   >
   > **`SASPortDisable`** ***`sas port`***

   If SAS ports A and B are used, then SAS ports C and D must be disabled. In the following example, the unused SAS ports C and D are disabled:

   ```
   Ready. *
   `SASPortDisable C`

   SAS Port C has been disabled.

   Ready. *
   `SASPortDisable D`

   SAS Port D has been disabled.

   Ready. *
   ```

   c. Save the bridge configuration:
   `SaveConfiguration`

   The following example shows that SAS ports C and D have been disabled. Note that the asterisk no longer appears, indicating that the configuration has been saved.

   ```
   Ready. *
   `SaveConfiguration`

   Ready.
   ```

2. Repeat the previous step on the bottom FC-to-SAS bridge.

Requirements for using other interfaces to configure and manage FibreBridge bridges

You can use the combination of a serial port, Telnet, and FTP to manage the FibreBridge bridges instead of the recommended management interfaces. Your system must meet the requirements for the applicable interface before you install the bridges.

You can use a serial port or Telnet to configure the bridge and Ethernet management 1 port, and to manage the bridge. You can use FTP to update the bridge firmware.

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

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

Serial port

When using the serial port to configure and manage a bridge, and to configure the Ethernet management 1 port, your system must meet the following requirements:

- A serial cable (which connects from the bridge serial port to a serial (COM) port on the computer you are using for setup)

  The bridge serial port is RJ-45 and has the same pin-out as the controllers.

- A terminal emulation program such as Hyperterminal, Teraterm, or PuTTY to access the console

  The terminal program should be capable of logging screen output to a file.

Telnet

When using Telnet to configure and manage a bridge, your system must meet the following requirements:

- A serial cable (which connects from the bridge serial port to a serial (COM) port on the computer you are using for setup)

  The bridge serial port is RJ-45 and has the same pin-out as the controllers.

- (Recommended) A non-default user name and password (for accessing the bridge)
- A terminal emulation program such as Hyperterminal, Teraterm, or PuTTY to access the console

  The terminal program should be capable of logging screen output to a file.

- An IP address, subnet mask, and gateway information for the Ethernet management 1 port on each bridge

FTP

When using FTP to update bridge firmware, your system must meet the following requirements:

- A standard Ethernet cable (which connects from the bridge Ethernet management 1 port to your network)
- (Recommended) A non-default user name and password (for accessing the bridge)

Hot-replacing a failed power supply module

When there is a change in status of a power supply module to the bridge, you can remove and install the power supply module.

You can view the change in status of a power supply module through the LEDs on the bridge. You can also view the status of power supply modules via ExpressNAV GUI and the bridge CLI, via serial port, or via Telnet.

- This procedure is NDO (non-disruptive) and takes approximately 15 minutes to complete.
- You need the admin password and access to an FTP or SCP server.

> 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.

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. Beginning with ONTAP 9.8, out-of-band management is deprecated.

> Starting with ONTAP 9.8, the **`storage bridge`** command is replaced with **`system bridge`**. The following steps show the **`storage bridge`** command, but if you are running ONTAP 9.8 or later, the **`system bridge`** command is preferred.

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.

The availability of in-band management of the bridges depends on the version of ONTAP:

- Starting with ONTAP 9.8, bridges are managed via in-band connections by default and out-of-band management of the bridges via SNMP is deprecated.
- ONTAP 9.5 through 9.7: Either in-band management or out-of-band SNMP management is supported.
- Prior to ONTAP 9.5, only out-of-band SNMP management is supported.

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.

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

Related information

Hot-swapping a bridge with a replacement bridge of the same model

Hot-swapping a FibreBridge 7500N with a 7600N bridge

[Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7600N or 7500N bridge]

[Hot-adding a stack of SAS disk shelves and bridges]

Managing a FibreBridge bridge from ONTAP

Starting with ONTAP 9.5, you can use the ONTAP CLI to pass FibreBridge commands to the bridge and display the results of those commands.

> Starting with ONTAP 9.8, the **`storage bridge`** command is replaced with **`system bridge`**. The following steps show the **`storage bridge`** command, but if you are running ONTAP 9.8 or later, the **`system bridge`** command is preferred.

Steps

1. Run the applicable FibreBridge command within the `storage bridge run-cli` command:

   `storage bridge run-cli -name` ***`bridge-name`*** **`-command`** ***`"command-text"`***

   The following command runs the FibreBridge `SASPortDisable` command from the ONTAP prompt to disable SAS port b on the bridge:

   ```
   cluster_A::> storage bridge run-cli -name "SASPortDisable b"

   SAS Port B has been disabled.
   Ready
   cluster_A::>
   ```

Securing or unsecuring the FibreBridge bridge

To easily disable potentially unsecure Ethernet protocols on a bridge, beginning with ONTAP 9.5 you can secure the bridge. This disables the bridge's Ethernet ports. You can also reenable Ethernet access.

- Securing the bridge disables telnet and other IP port protocols and services (FTP, ExpressNAV, ICMP, or QuickNAV) on the bridge.
- This procedure uses out-of-band management using the ONTAP prompt, which is available beginning with ONTAP 9.5.

  You can issue the commands from the bridge CLI if you are not using out-of-band management.
- The **`unsecurebridge`** command can be used to reenable the Ethernet ports.
- In ONTAP 9.7 and earlier, running the **`securebridge`** command on the ATTO FibreBridge might not update the bridge status correctly on the partner cluster. If this occurs, run the **`securebridge`** command from the partner cluster.

Starting with ONTAP 9.8, the **storage bridge** command is replaced with **system bridge**. The following steps show the **storage bridge** command, but if you are running ONTAP 9.8 or later, the **system bridge** command is preferred.

Steps

1. From the ONTAP prompt of the cluster containing the bridge, secure or unsecure the bridge.

   The following command secures bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   securebridge
   ```

   The following command unsecures bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   unsecurebridge
   ```

2. From the ONTAP prompt of the cluster containing the bridge, save the bridge configuration:

   storage bridge run-cli -bridge *bridge-name* -command saveconfiguration

   The following command secures bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   saveconfiguration
   ```

3. From the ONTAP prompt of the cluster containing the bridge, restart the bridge's firmware:

   storage bridge run-cli -bridge *bridge-name* -command firmwarerestart

   The following command secures bridge_A_1:

   ```
   cluster_A> storage bridge run-cli -bridge bridge_A_1 -command
   firmwarerestart
   ```

Performing FC switch maintenance and replacement

If necessary, you can non-disruptively replace the FC switches or upgrade their firmware in the MetroCluster configuration.

Upgrading or downgrading the firmware on a Brocade FC switch

To upgrade or downgrade the firmware on a Brocade FC switch, you must use the

Brocade-specific commands to disable the switch, perform and verify the firmware change, and reboot and reenable the switch.

- You must have the firmware files.
- The system must be properly cabled.
- All paths to the storage shelves must be available.
- The disk shelf stacks must be stable.
- The FC switch fabric must be healthy.
- No failed components can be present in the system.
- The system must be operating normally.
- You must have the admin password and access to an FTP or SCP server.

The switch fabric is disabled during a firmware upgrade or downgrade, and the MetroCluster configuration relies on the second fabric to continue operation.

This task must be performed on each of the switch fabrics in succession so that all switches are running the same firmware version.

> This procedure is nondisruptive and takes approximately one hour to complete.

Steps

1. Log in to each of the switches in the fabric.

   The examples in the following steps use the switch `FC_switch_A_1`.

2. Disable each of the switches in the fabric:

   `switchCfgPersistentDisable`

   If this command is not available, then run the `switchDisable` command.

   ```
   FC_switch_A_1:admin> switchCfgPersistentDisable
   ```

3. Download the desired firmware version:

   `firmwareDownload`

   When prompted for the file name, you must specify the subdirectory or relative path to the firmware file.

   You can run the `firmwareDownload` command at the same time on both switches, but you must allow the firmware to download and commit properly before moving to the next step.

```
FC_switch_A_1:admin> firmwaredownload
Server Name or IP Address: 10.64.203.188
User Name: test
File Name: v7.3.1b
Network Protocol(1-auto-select, 2-FTP, 3-SCP, 4-SFTP) [1]: 2
Password:
Server IP: 10.64.203.188, Protocol IPv4
Checking system settings for firmwaredownload...
System settings check passed.
```

4. Verify that the firmware was downloaded and committed to both partitions:

   `firmwareShow`

   The following example shows that the firmware download is complete as both images are updated:

```
FC_switch_A_1:admin> firmwareShow
Appl     Primary/Secondary Versions

------------------------------------------

FOS      v7.3.1b

         v7.3.1b
```

5. Reboot the switches:

   `reboot`

   Some firmware versions automatically perform an haReboot operation after the firmware download is finished. The reboot in this step is required even if the haReboot has been performed.

```
FC_switch_A_1:admin> reboot
```

6. Check whether the new firmware is for an intermediate firmware level or for a final specified release.

   If the download is for the intermediate firmware level, then perform the previous two steps until the specified release is installed.

7. Enable the switches:

   `switchCfgPersistentEnable`

   If this command is not available, then the switch should be in the `enabled` state after the `reboot` command is executed.

```
FC_switch_A_1:admin> switchCfgPersistentEnable
```

8. Verify that the switches are online and that all of the devices are properly logged in:

   `switchShow`

   ```
   FC_switch_A_1:admin> switchShow
   ```

9. Verify that the buffer usage information for a port group or all of the port groups in the switch is displayed properly:

   `portbuffershow`

   ```
   FC_switch_A_1:admin> portbuffershow
   ```

10. Verify that the current configuration of a port is displayed properly:

    `portcfgshow`

    ```
    FC_switch_A_1:admin> portcfgshow
    ```

    Verify the port settings, such as speed, mode, trunking, encryption, and compression, in the Inter-Switch Link (ISL) output. Verify that the port settings were not affected by the firmware download.

11. Verify the operation of the MetroCluster configuration in ONTAP:

    a. Check whether the system is multipathed:
       `node run -node` ***`node-name`*** **`sysconfig -a`**

    b. Check for any health alerts on both clusters:
       `system health alert show`

    c. Confirm the MetroCluster configuration and that the operational mode is normal:
       `metrocluster show`

    d. Perform a MetroCluster check:
       `metrocluster check run`

    e. Display the results of the MetroCluster check:
       `metrocluster check show`

    f. Check for any health alerts on the switches (if present):
       `storage switch show`

    g. Run Config Advisor.

       NetApp Downloads: Config Advisor

    h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

12. Wait 15 minutes before repeating this procedure for the second switch fabric.

Upgrading or downgrading the firmware on a Cisco FC switch

To upgrade or downgrade the firmware on a Cisco FC switch you must use the Cisco-specific commands to disable the switch, perform and verify the upgrade, and reboot and reenable the switch.

- The system must be properly cabled.
- All paths to the storage shelves must be available.
- The disk shelf stacks must be stable.
- The FC switch fabric must be healthy.
- All components in the system must be healthy.
- The system must be operating normally.
- You need the admin password and access to an FTP or SCP server.

The switch fabric is disabled during the firmware upgrade or downgrade and the MetroCluster configuration relies on the second fabric to continue operation.

You must repeat this task on each of the switch fabrics in succession to ensure that all switches are running the same firmware version.

You must have the firmware files.

> This procedure is nondisruptive and takes approximately one hour to complete.

Steps

1. Log in to each of the switches in the fabric.

   In the examples, the switches are called FC_switch_A_1 and FC_switch_B_1.

2. Determine whether there is enough space in the bootflash directory on each switch:

   `dir bootflash`

   If not, delete the unwanted firmware files by using the `delete bootflash:file_name` command.

3. Copy the kickstart and system files to the switches:

   `copy` ***`source_filetarget_file`***

   In the following example, the kickstart file (`m9200-s2ek9-kickstart-mz.5.2.1.bin`) and the system file (`m9200-s2ek9-mz.5.2.1.bin`) are located on the FTP server 10.10.10.55 in the `/firmware/` path.

   The following example shows the commands issued on FC_switch_A_1:

```
FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-kickstart-
mz.5.2.1.bin bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
FC_switch_A_1# copy ftp://10.10.10.55/firmware/m9200-s2ek9-mz.5.2.1.bin
bootflash:m9200-s2ek9-mz.5.2.1.bin
```

4. Disable all the VSANs on both the switches in this fabric.
5. Install the desired firmware on the switches:

   `install all system bootflash:`*`systemfile_name`*` kickstart bootflash:`*`kickstartfile_name`*

   The following example shows the commands issued on FC_switch_A_1:

   ```
   FC_switch_A_1# install all system bootflash:m9200-s2ek9-mz.5.2.1.bin
   kickstart bootflash:m9200-s2ek9-kickstart-mz.5.2.1.bin
   Enter Yes to confirm the installation.
   ```

6. Check the version of the firmware on each switch to make sure the correct version was installed:

   `show version`

7. Enable all the VSANs on both the switches in this fabric.
8. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed: + **`node run -node`** ***`node-name`*** **`sysconfig -a`**
   b. Check for any health alerts on both clusters: + **`system health alert show`**
   c. Confirm the MetroCluster configuration and that the operational mode is normal: + **`metrocluster show`**
   d. Perform a MetroCluster check: + **`metrocluster check run`**
   e. Display the results of the MetroCluster check: + **`metrocluster check show`**
   f. Check for any health alerts on the switches (if present): + **`storage switch show`**
   g. Run Config Advisor.

      NetApp Downloads: Config Advisor

   h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
9. Repeat this procedure for the second switch fabric.

Upgrading to new Brocade FC switches

If you are upgrading to new Brocade FC switches, you must replace the switches in the first fabric, verify that the MetroCluster configuration is fully operational, and then replace the switches in the second fabric.

- The MetroCluster configuration must be healthy and in normal operation.
- The MetroCluster switch fabrics consist of four Brocade switches.

  The illustrations in the following steps show current switches.

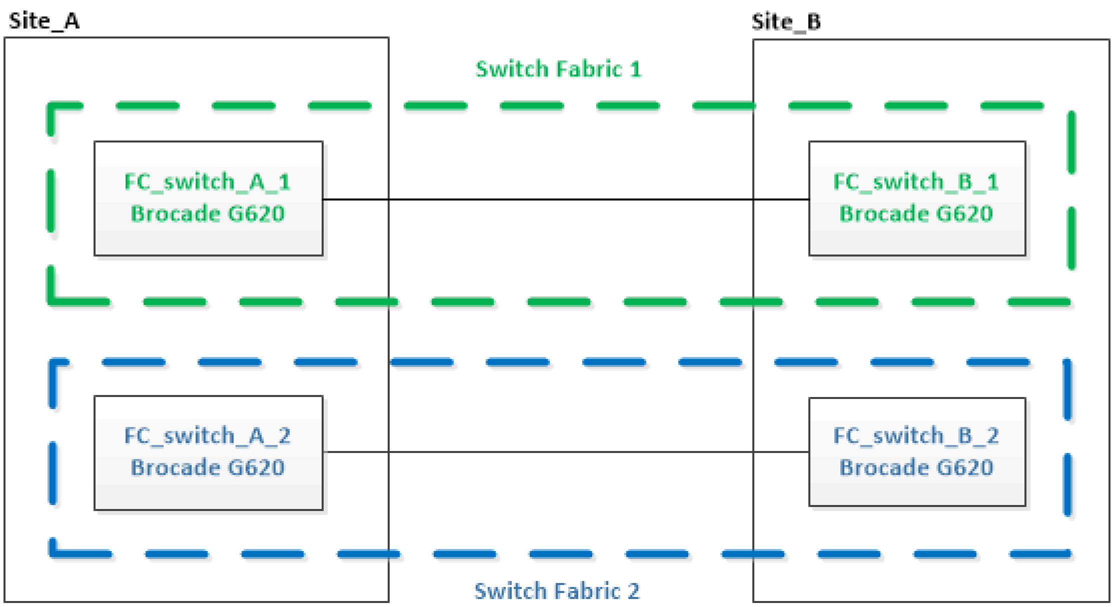
- The switches must be running the most recent supported firmware.

  NetApp Interoperability Matrix Tool

- This procedure is nondisruptive and takes approximately two hours to complete.
- You need the admin password and access to an FTP or SCP server.

The switch fabrics are upgraded one at a time.

At the end of this procedure, all four switches will be upgraded to new switches.

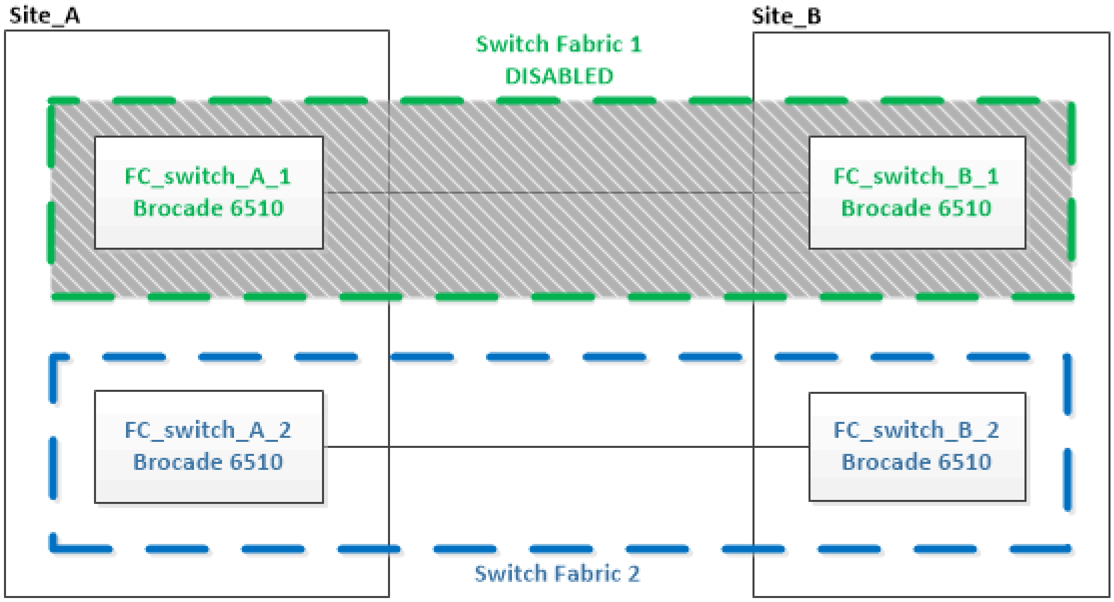


Steps

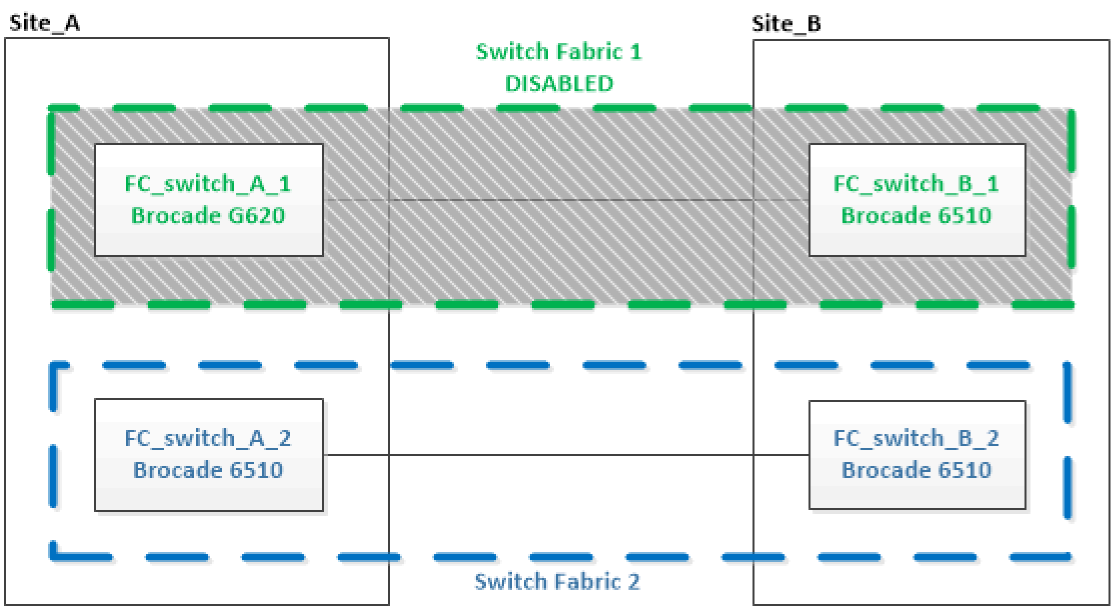
1. Disable the first switch fabric:

   `FC_switch_A_1:admin> switchCfgPersistentDisable`

```
FC_switch_A_1:admin> switchCfgPersistentDisable
```



2. Replace the old switches at one MetroCluster site.
   a. Uncable and remove the disabled switch.
   b. Install the new switch in the rack.



   c. Disable the new switches:
   `switchCfgPersistentDisable`

   The command disables both switches in the switch fabric.

```
FC_switch_A_1:admin> switchCfgPersistentDisable
```

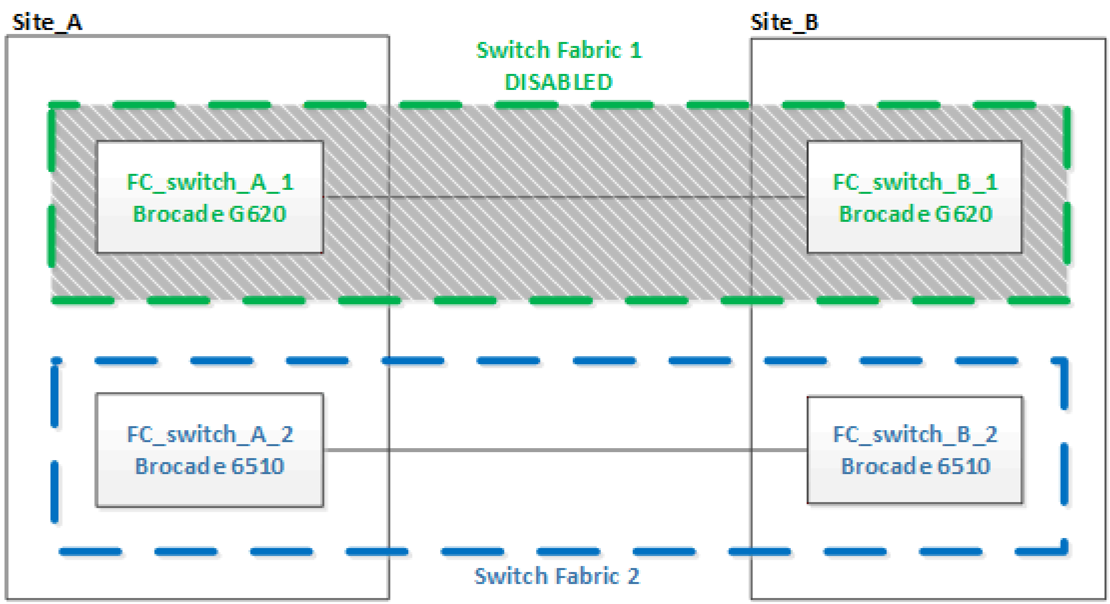
   d. Cable the new switch using the recommended port assignments.

   Port assignments for FC switches when using ONTAP 9.0

[Port assignments for FC switches when using ONTAP 9.1 and later]

e. Repeat these substeps at the partner MetroCluster site to replace the second switch in the first switch fabric.

   Both switches in fabric 1 have been replaced.



3. Power up the new switches and let them boot up.
4. Download the RCF files for the new switch.
5. Apply the RCF files to both new switches in the fabric, following the directions on the download page.
6. Save the switch configuration:

   cfgSave

7. Wait 10 minutes to allow the configuration to stabilize.
8. Confirm connectivity to the disks by entering the following command on any one of the MetroCluster nodes:

   run local sysconfig -v

   The output shows the disks attached to the initiator ports on the controller, and identifies the shelves connected to the FC-to-SAS bridges:

```
node_A_1> run local sysconfig -v
NetApp Release 9.3.2X18: Sun Dec 13 01:23:24 PST 2017
System ID: 4068741258 (node_A_1); partner ID: 4068741260 (node_B_1)
System Serial Number: 940001025471 (node_A_1)
System Rev: 70
System Storage Configuration: Multi-Path HA**<=== Configuration should
be multi-path HA**
.
.
.
```

```
slot 0: FC Host Adapter 0g (QLogic 8324 rev. 2, N-port, <UP>)**<===
Initiator port**
        Firmware rev:      7.5.0
        Flash rev:         0.0.0
        Host Port Id:      0x60130
        FC Node Name:      5:00a:098201:bae312
        FC Port Name:      5:00a:098201:bae312
        SFP Vendor:        UTILITIES CORP.
        SFP Part Number:   FTLF8529P3BCVAN1
        SFP Serial Number: URQ0Q9R
        SFP Capabilities:  4, 8 or 16 Gbit
        Link Data Rate:    16 Gbit
        Switch Port:       brcd6505-fcs40:1
  **<List of disks visible to port\>**
         ID     Vendor   Model            FW    Size
        brcd6505-fcs29:12.126L1527     : NETAPP   X302_HJUPI01TSSM NA04
847.5GB (1953525168 512B/sect)
        brcd6505-fcs29:12.126L1528     : NETAPP   X302_HJUPI01TSSA NA02
847.5GB (1953525168 512B/sect)
        .
        .
        .
        **<List of FC-to-SAS bridges visible to port\>**
        FC-to-SAS Bridge:
        brcd6505-fcs40:12.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:13.126L0        : ATTO     FibreBridge6500N 1.61
FB6500N102980
        brcd6505-fcs42:6.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N101167
        brcd6505-fcs42:7.126L0         : ATTO     FibreBridge6500N 1.61
FB6500N102974
        .
        .
        .
  **<List of storage shelves visible to port\>**
        brcd6505-fcs40:12.shelf6: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        brcd6505-fcs40:12.shelf8: DS4243  Firmware rev. IOM3 A: 0200
IOM3 B: 0200
        .
        .
        .
```

9. Returning to the switch prompt, verify the switch firmware version:

firmwareShow

The switches must be running the most recent supported firmware.

NetApp Interoperability Matrix Tool

10. Simulate a switchover operation:

    a. From any node's prompt, change to the advanced privilege level:
       set -privilege advanced

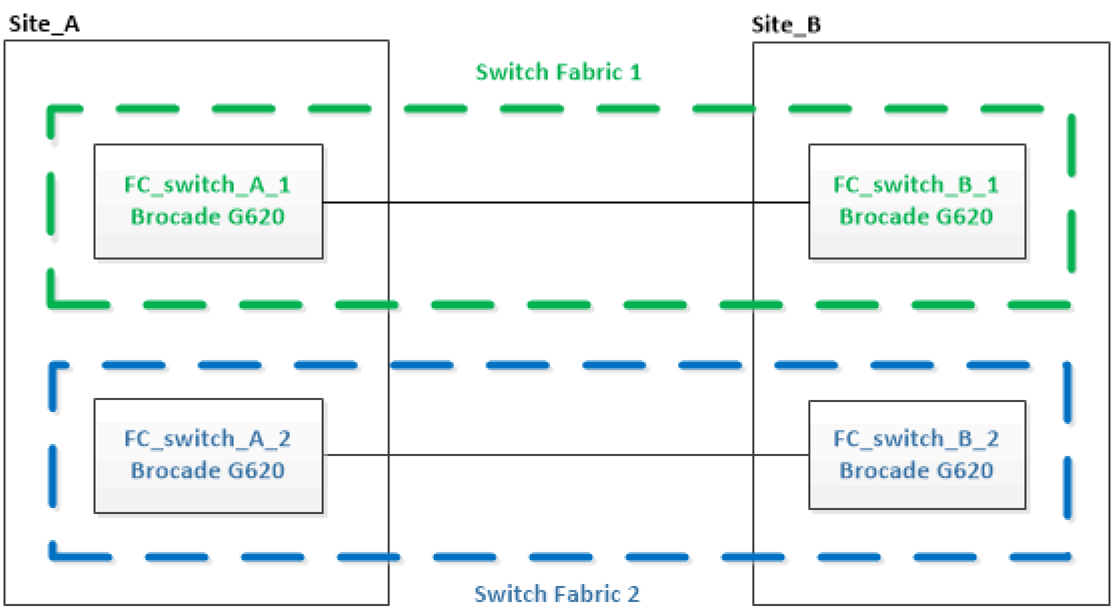
       You need to respond with **y** when prompted to continue into advanced mode and see the advanced mode prompt (*>).

    b. Perform the switchover operation with the `-simulate` parameter:
       metrocluster switchover -simulate

    c. Return to the admin privilege level:
       set -privilege admin

11. Repeat the previous steps on the second switch fabric.

After repeating the steps, all four switches have been upgraded and the MetroCluster configuration is in normal operation.



Replacing a Brocade FC switch

You must use this Brocade-specific procedure to replace a failed switch.

You need the admin password and access to an FTP or SCP server.

In the following examples, FC_switch_A_1 is the healthy switch and FC_switch_B_1 is the impaired switch. The switch port usage in the examples is shown in the following table:

Port connections	Ports
FC-VI connections	0, 3
HBA connections	1, 2, 4, 5
FC-to-SAS bridge connections	6, 7
ISL connections	10, 11

The examples show two FC-to-SAS bridges. If you have more, you must disable and subsequently enable the additional ports.

> ⓘ This procedure is nondisruptive and takes approximately two hours to complete.

Your switch port usage should follow the recommended assignments.

- Port assignments for FC switches when using ONTAP 9.0
- Port assignments for FC switches when using ONTAP 9.1 and later

Steps

1. Fence off the switch undergoing replacement by disabling the ISL ports on the healthy switch in the fabric and the FC-VI and HBA ports on the impaired switch (if the impaired switch is still operating):

   a. Disable the ISL ports on the healthy switch for each port:
   `portcfgpersistentdisable` ***`port-number`***

   ```
   FC_switch_A_1:admin> portcfgpersistentdisable 10
   FC_switch_A_1:admin> portcfgpersistentdisable 11
   ```

   b. If the impaired switch is still operational, disable the FC-VI and HBA ports on that switch for each port:
   `portcfgpersistentdisable` ***`port-number`***

   ```
   FC_switch_B_1:admin> portcfgpersistentdisable 0
   FC_switch_B_1:admin> portcfgpersistentdisable 1
   FC_switch_B_1:admin> portcfgpersistentdisable 2
   FC_switch_B_1:admin> portcfgpersistentdisable 3
   FC_switch_B_1:admin> portcfgpersistentdisable 4
   FC_switch_B_1:admin> portcfgpersistentdisable 5
   ```

2. If the impaired switch is still operational, gather the output from the **`switchshow`** command.

```
FC_switch_B_1:admin> switchshow
    switchName: FC_switch_B_1
    switchType: 71.2
    switchState:Online
    switchMode: Native
    switchRole: Subordinate
    switchDomain:       2
    switchId:   fffc01
    switchWwn:  10:00:00:05:33:86:89:cb
    zoning:             OFF
    switchBeacon:       OFF
```

3. Boot and preconfigure the new switch prior to physically installing it:
   a. Power up the new switch and let it boot up.
   b. Check the firmware version on the switch to confirm that it matches the version of the other FC switches:
      firmwareShow
   c. Configure the new switch as described in the *MetroCluster Installation and Configuration Guide*, but skipping the "Configuring zoning on Brocade FC switches" section.

      Fabric-attached MetroCluster installation and configuration

      You configure zoning later in this procedure.

      At this point, the new switch is not cabled to the MetroCluster configuration.

   d. Disable the FC-VI, HBA, and storage ports on the new switch, and the ports connected to the FC-SAS bridges.

```
FC_switch_B_1:admin> portcfgpersistentdisable 0
FC_switch_B_1:admin> portcfgpersistentdisable 1
FC_switch_B_1:admin> portcfgpersistentdisable 2
FC_switch_B_1:admin> portcfgpersistentdisable 3
FC_switch_B_1:admin> portcfgpersistentdisable 4
FC_switch_B_1:admin> portcfgpersistentdisable 5

FC_switch_B_1:admin> portcfgpersistentdisable 6
FC_switch_B_1:admin> portcfgpersistentdisable 7
```

4. Physically replace the switch:
   a. Power off the impaired FC switch.
   b. Power off the replacement FC switch.
   c. Uncable and remove the impaired switch, carefully noting which cables connected to which ports.
   d. Install the replacement switch in the rack.

e. Cable the replacement switch exactly as the old switch was cabled.

f. Power on the new FC switch.

5. If you want to enable ISL encryption, complete the applicable tasks in the Fabric-attached MetroCluster Installation and Configuration Guide.

   If you are enabling ISL encryption, you need to complete the following tasks:

   - Disabling the virtual fabric
   - Setting the payload
   - Setting the authentication policy
   - Enabling ISL encryption on Brocade switches

6. Complete the configuration of the new switch:

   a. Enable the ISLs:
   portcfgpersistentenable *port-number*

```
FC_switch_B_1:admin> portcfgpersistentenable 10
FC_switch_B_1:admin> portcfgpersistentenable 11
```

   b. On the replacement switch (FC_switch_B_1 in the example), verify that the ISLs are online:
   switchshow

```
FC_switch_B_1:admin> switchshow
switchName: FC_switch_B_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online   FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1"
11   11    030B00 id   16G     Online   FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)
...
```

   c. Enable the storage ports that connect to the FC bridges.

```
FC_switch_B_1:admin> portcfgpersistentenable 6
FC_switch_B_1:admin> portcfgpersistentenable 7
```

d. Enable the storage, HBA, and FC-VI ports.

The following example shows the commands used to enable the ports connecting HBA adapters:

```
FC_switch_B_1:admin> portcfgpersistentenable 1
FC_switch_B_1:admin> portcfgpersistentenable 2
FC_switch_B_1:admin> portcfgpersistentenable 4
FC_switch_B_1:admin> portcfgpersistentenable 5
```

The following example shows the commands used to enable the ports connecting the FC-VI adapters:

```
FC_switch_B_1:admin> portcfgpersistentenable 0
FC_switch_B_1:admin> portcfgpersistentenable 3
```

7. Verify that the ports are online:

   switchshow

8. Verify the operation of the MetroCluster configuration in ONTAP:

   a. Check whether the system is multipathed:
   node run -node *node-name* sysconfig -a

   b. Check for any health alerts on both clusters:

   system health alert show

   c. Confirm the MetroCluster configuration and that the operational mode is normal:

   metrocluster show

   d. Perform a MetroCluster check:

   metrocluster check run

   e. Display the results of the MetroCluster check:

   metrocluster check show

   f. Check for any health alerts on the switches (if present):

   storage switch show

   g. Run Config Advisor.

   NetApp Downloads: Config Advisor

h. After running Config Advisor, review the tool’s output and follow the recommendations in the output to address any issues discovered.

Renaming a Brocade FC switch

You might need to rename a Brocade FC switch to ensure consistent naming throughout your configuration.

Steps

1. Persistently disable the switch or switches in one fabric:

   `switchcfgpersistentdisable`

   The following example shows the output for the **`switchcfgpersistentdisable`** command:

   ```
   7840_FCIP_2:admin> switchcfgpersistentdisable
   Switch's persistent state set to 'disabled'
   2018/03/09-07:41:06, [ESM-2105], 146080, FID 128, INFO, 7840_FCIP_2, VE
   Tunnel 24 is DEGRADED.
   2018/03/09-07:41:06, [ESM-2104], 146081, FID 128, INFO, 7840_FCIP_2, VE
   Tunnel 24 is OFFLINE.

   7840_FCIP_2:admin>
   ```

2. Rename the switch or switches:

   `switchname` ***`new-switch-name`***

   If you are renaming both switches in the fabric, use the same command on each switch.

   The following example shows the output for the **`switchname`** ***`new-switch-name`*** command:

   ```
   7840_FCIP_2:admin> switchname FC_switch_1_B
   Committing configuration...
   Done.
   Switch name has been changed.Please re-login into the switch for the
   change to be applied.
   2018/03/09-07:41:20, [IPAD-1002], 146082, FID 128, INFO, FC_switch_1_B,
   Switch name has been successfully changed to FC_switch_1_B.
   7840_FCIP_2:admin>
   ```

3. Reboot the switch or switches:

   `reboot`

   If you are renaming both switches in the fabric, reboot both switches. Once the reboot is complete, the switch is renamed in all places.

The following example shows the output for the **reboot** command:

```
7840_FCIP_2:admin> reboot
Warning: This command would cause the switch to reboot
and result in traffic disruption.
Are you sure you want to reboot the switch [y/n]?y
2018/03/09-07:42:08, [RAS-1007], 146083, CHASSIS, INFO, Brocade7840,
System is about to reload.
Rebooting! Fri Mar  9 07:42:11 CET 2018

Broadcast message from root (ttyS0) Fri Mar  9 07:42:11 2018...

The system is going down for reboot NOW !!
INIT: Switching to runlevel: 6
INIT:
2018/03/09-07:50:48, [ESM-1013], 146104, FID 128, INFO, FC_switch_1_B,
DP0 Configuration replay has completed.
2018/03/09-07:50:48, [ESM-1011], 146105, FID 128, INFO, FC_switch_1_B,
DP0 is ONLINE.

*** CORE FILES WARNING (03/09/18 - 08:00:00 ) ***
10248 KBytes in 1 file(s)
use "supportsave" command to upload


*** FFDC FILES WARNING (03/09/18 - 08:00:00 ) ***
520 KBytes in 1 file(s)
```

4. Persistently enable the switches: **switchcfgpersistentenable**

   The following example shows the output for the **switchcfgpersistentenable** command:

```
FC_switch_1_B:admin> switchcfgpersistentenable
Switch's persistent state set to 'enabled'
FC_switch_1_B:admin>
FC_switch_1_B:admin>
FC_switch_1_B:admin> 2018/03/09-08:07:07, [ESM-2105], 146106, FID 128,
INFO, FC_switch_1_B, VE Tunnel 24 is DEGRADED.
2018/03/09-08:07:10, [ESM-2106], 146107, FID 128, INFO, FC_switch_1_B,
VE Tunnel 24 is ONLINE.

FC_switch_1_B:admin>


FC_switch_1_B:admin> switchshow
switchName:     FC_switch_1_B
switchType:     148.0
switchState:    Online
switchMode:     Native
switchRole:     Subordinate
switchDomain:   6
switchId:       fffc06
switchWwn:      10:00:50:eb:1a:9a:a5:79
zoning:         ON (CFG_FAB_2_RCF_9_3)
switchBeacon:   OFF
FC Router:      OFF
FC Router BB Fabric ID: 128
Address Mode:   0
HIF Mode:       OFF

Index Port Address  Media Speed   State       Proto
==================================================
   0   0   060000   id    16G     Online      FC  F-Port
50:0a:09:81:06:a5:5a:08
   1   1   060100   id    16G     Online      FC  F-Port
50:0a:09:83:06:a5:5a:08
```

5. Verify that the switch name change is visible from the ONTAP cluster prompt:

   `storage switch show`

   The following example shows the output for the **`storage switch show`** command:

```
cluster_A::*> storage switch show
  (storage switch show)
                      Symbolic                                Is
Monitor
Switch                Name     Vendor  Model Switch WWN       Monitored
Status
--------------------- -------- ------- ----- ---------------- ---------
-------
Brocade_172.20.7.90
                      RTP-FC01-510Q40
                               Brocade Brocade7840
                                             1000c4f57c904bc8 true
ok
Brocade_172.20.7.91
                      RTP-FC02-510Q40
                               Brocade Brocade7840
                                             100050eb1a9aa579 true
ok
Brocade_172.20.7.92
```

Disabling encryption on Brocade FC switches

You might need to disable encryption on Brocade FC switches.

Steps

1. Send an AutoSupport message from both sites indicating the beginning of maintenance.

```
cluster_A::> autosupport invoke -node * -type all -message MAINT=4h
```

```
cluster_B::> autosupport invoke -node * -type all -message MAINT=4h
```

2. Verify the operation of the MetroCluster configuration from Cluster A.

   a. Confirm the MetroCluster configuration and that the operational mode is normal:
   `metrocluster show`

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

   b. Perform a MetroCluster check:
   `metrocluster check run`

```
cluster_A::> metrocluster check run
```

c. Display the results of the MetroCluster check:
`metrocluster check show`

```
cluster_A::> metrocluster check show
```

3. Check the status of both switches:

   `fabric show`

```
switch_A_1:admin> fabric show
```

```
switch_B_1:admin> fabric show
```

4. Disable both switches:

   `switchdisable`

```
switch_A_1:admin> switchdisable
```

```
switch_B_1:admin> switchdisable
```

5. Check the available paths for the nodes on each cluster:

   `sysconfig`

```
cluster_A::> system node run -node node-name -command sysconfig -a
```

```
cluster_B::> system node run -node node-name -command sysconfig -a
```

   As the switch fabric is now disabled, the System Storage Configuration should be Single-Path HA.

6. Check the aggregate status for both clusters.

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

System output should show the aggregates are mirrored and normal for both clusters:

```
mirrored,normal
```

7. Repeat the following substeps from the admin prompt on both switches.

   a. Show which ports are encrypted:
   `portenccompshow`

   ```
   switch_A_1:admin> portenccompshow
   ```

   b. Disable encryption on the encrypted ports:
   `portcfgencrypt – disable` ***`port-number`***

   ```
   switch_A_1:admin> portcfgencrypt --disable 40
   switch_A_1:admin> portcfgencrypt --disable 41
   switch_A_1:admin> portcfgencrypt --disable 42
   switch_A_1:admin> portcfgencrypt --disable 43
   ```

   c. Set the authentication type to all:

   `authUtil --set -a all`

   ```
   switch_A_1:admin> authUtil --set -a all
   ```

   d. Set the authentication policy on the switch. to off:
   `authutil --policy -sw off`

   ```
   switch_A_1:admin> authutil --policy -sw off
   ```

   e. Set the authentication Diffie-Hellman group to * :
   `authutil --set -g *`

   ```
   switch_A_1:admin> authUtil --set -g *
   ```

   f. Delete the secret key database:
   `secAuthSecret --remove -all`

```
switch_A_1:admin> secAuthSecret --remove -all
```

g. Confirm that encryption is disabled on the ports:
portenccompshow

```
switch_A_1:admin> portenccompshow
```

h. Enable the switch:
switchenable

```
switch_A_1:admin> switchenable
```

i. Confirm the status of the ISLs:
islshow

```
switch_A_1:admin> islshow
```

8. Check the available paths for the nodes on each cluster:

   sysconfig

```
cluster_A::> system node run -node * -command sysconfig -a
```

```
cluster_B::> system node run -node * -command sysconfig -a
```

   The system output should indicate that System Storage Configuration has changed back to Quad-Path HA.

9. Check the aggregate status for both clusters.

```
cluster_A::> aggr status
```

```
cluster_B::> aggr status
```

   The system should show that the aggregates are mirrored and normal for both clusters as shown in the following system output:

```
mirrored,normal
```

10. Verify the operation of the MetroCluster configuration from Cluster A.

    a. Perform a MetroCluster check:
    `metrocluster check run`

    ```
    cluster_A::> metrocluster check run
    ```

    b. Display the results of the MetroCluster check:
    `metrocluster check show`

    ```
    cluster_A::> metrocluster check show
    ```

11. Send an AutoSupport message from both sites indicating the end of maintenance.

    ```
    cluster_A::> autosupport invoke -node node-name -type all -message
    MAINT=END
    ```

    ```
    cluster_B::> autosupport invoke -node node-name -type all -message
    MAINT=END
    ```

Changing ISL properties, ISL ports, or the IOD/OOD configuration on a Brocade switch

You might need to add ISLs to a switch if you are adding or upgrading hardware such as additional or faster controllers or switches.

Ensure that the system is properly configured, that all fabric switches are operational, and that no errors exist.

If the equipment on the ISL link changes and the new link configuration no longer supports the current configuration----trunking and ordered delivery----then the fabric needs to be reconfigured for the correct routing policy: either in-order-deliver (IOD) or out-of-order-delivery (OOD).

> To make changes to OOD from ONTAP software, use the following steps: Configuring in-order delivery or out-of-order delivery of frames on ONTAP software

Steps

1. Disable the FCVI and storage HBA ports:

   `portcfgpersistentdisable` ***`port number`***

   By default the first 8 ports (ports 0 through 7) are used for FCVI and Storage HBA. The ports must be persistently disabled so that the ports remain disabled in the event of a switch reboot.

   The following example shows ISL ports 0—7 being disabled on both switches:

```
Switch_A_1:admin> portcfgpersistentdisable 0-7
Switch_B_1:admin> portcfgpersistentdisable 0-7
```

2. Change the ISL ports as required.

Option	Step

To change the speed of an ISL port…	Use the **`portcfgspeed`** ***`port number port speed`*** command on both switches on the fabric.
	
	In the following example, you change the ISL port speed from 40 Gbps to 16 Gbps:
	
	`brocade_switch_A_1:admin> portcfgspeed 40 16`
	
	You can verify that the speed has changed using the `switchshow` command:
	
	`brocade_switch_A_1:admin> switchshow`
	
	You should see the following output:
	
	`. . .`
	`40  40  062800  id`
	`16G  No_Sync  FC  Disabled`
	`. . .`

To change the distance of an ISL port…	Use the **`portcfglongdistance`** ***`port number port distance`*** command on both switches in the fabric.
To remove an ISL…	Disconnect the link \(cable\).
To add an ISL…	Insert SFPs into the ports you are adding as ISL ports. Ensure that these ports are listed in the **Fabric-attached MetroCluster Installation and Configuration Guide** for the switch you are adding them to and cable them according to this guide.
To relocate an ISL…	Relocating an ISL is the same as removing and then adding an ISL. First, remove the ISL by disconnecting the link and then insert SFPs into the ports you are adding as ISL ports.

3. Reconfigure for out-of-order delivery (OOD) or in-order-delivery (IOD).

> If the routing policies remain the same, you do not need to reconfigure and this step can be ignored. The ONTAP configuration needs to match the fabric configuration. If the fabric is configured for OOD, then ONTAP must also be configured for OOD. The same applies for IOD.

This step should be executed in the following scenarios:

- More than one ISL formed a trunk before the change, but after the change, trunking is no longer supported. In this case, you must configure the fabric for OOD.
- There is one ISL before the change and multiple ISLs after the change.
- If multiple ISLs form a trunk, configure the fabric for IOD. If multiple ISLs **cannot** form a trunk, configure the fabric for OOD.
- Persistently disable the switches using the **`switchcfgpersistentdisable`** command as shown in the following example:

```
Switch_A_1:admin> switchcfgpersistentdisable
Switch_B_1:admin> switchcfgpersistentdisable
```

a. Configure the trunking mode for each ISL **`portcfgtrunkport`** ***`port number`*** as shown in the following table:

Scenario	Steps

Configure the ISL for trunking \(IOD\)	Set the **`portcfgtrunkport`** ***`port number`*** to 1:
	`FC_switch_A_1:admin> portcfgtrunkport 20 1`
	`FC_switch_A_1:admin> portcfgtrunkport 21 1`
	`FC_switch_B_1:admin> portcfgtrunkport 20 1`
	`FC_switch_B_1:admin> portcfgtrunkport 21 1`

Scenario	**Steps**

Configure the ISL for trunking \(OOD\)	Set the **`portcfgtrunkport`** ***`port number`*** `to 0:`
	 <pre>FC_switch_A_1:admin>
	portcfgtrunkport 20 0
	FC_switch_A_1:admin>
	portcfgtrunkport 21 0
	FC_switch_B_1:admin>
	portcfgtrunkport 20 0
	FC_switch_B_1:admin>
	portcfgtrunkport 21 0
	``</pre>

b. Configure the fabric for IOD or OOD as required.

Scenario	Steps

Configure the fabric for IOD	Set the three settings of IOD, APT, and DLS using the **`iodset`**, **`aptpolicypolicy`**, and **`dlsreset`** commands as shown in the following example:
	 <pre>Switch_A_1:admin> iodset
	Switch_A_1:admin> aptpolicy 1
	Policy updated successfully.
	Switch_A_1:admin> dlsreset
	FC_switch_A_1:admin>portcfgtru
	nkport 40 1
	FC_switch_A_1:admin>portcfgtru
	nkport 41 1</pre> <pre>Switch_B_1:admin> iodset
	Switch_B_1:admin> aptpolicy 1
	Policy updated successfully.
	Switch_B_1:admin> dlsreset
	FC_switch_B_1:admin>portcfgtru
	nkport 20 1
	FC_switch_B_1:admin>portcfgtru
	nkport 21 1</pre>

Configure the fabric for OOD	Set the three settings of IOD, APT, and DLS using the **iodreset**, **aptpolicy*policy***, and **dlsset** commands as shown in the following example:
	
	`Switch_A_1:admin> iodreset`
	`Switch_A_1:admin> aptpolicy 3`
	`Policy updated successfully.`
	`Switch_A_1:admin> dlsset`
	`FC_switch_A_1:admin>`
	`portcfgtrunkport 40 0`
	`FC_switch_A_1:admin>`
	`portcfgtrunkport 41 0`
	
	`Switch_B_1:admin> iodreset`
	`Switch_B_1:admin> aptpolicy 3`
	`Policy updated successfully.`
	`Switch_B_1:admin> dlsset`
	`FC_switch_B_1:admin>`
	`portcfgtrunkport 40 0`
	`FC_switch_B_1:admin>`
	`portcfgtrunkport 41 0`

c. Enable the switches persistently using the **switchcfgpersistentenable** command.

```
switch_A_1:admin>switchcfgpersistentenable
switch_B_1:admin>switchcfgpersistentenable
```

If this command does not exist, use the `switchenable` command as shown in the following example:

```
brocade_switch_A_1:admin>
switchenable
```

d. Verify the OOD settings using the **iodshow**, **aptpolicy**, and **dlsshow** commands as shown in the following example:

```
switch_A_1:admin> iodshow
IOD is not set

switch_A_1:admin> aptpolicy

                Current Policy: 3 0(ap)

                3 0(ap) : Default Policy
                1: Port Based Routing Policy
                3: Exchange Based Routing Policy
                     0: AP Shared Link Policy
                     1: AP Dedicated Link Policy
                command aptpolicy completed

switch_A_1:admin> dlsshow
DLS is set by default with current routing policy
```

> You must run these commands on both switches.

e. Verify the IOD settings using the **`iodshow`**, **`aptpolicy`**, and **`dlsshow`** commands as shown in the following example:

```
switch_A_1:admin> iodshow
IOD is set

switch_A_1:admin> aptpolicy
                    Current Policy: 1 0(ap)

                    3 0(ap) : Default Policy
                    1: Port Based Routing Policy
                    3: Exchange Based Routing Policy
                         0: AP Shared Link Policy
                         1: AP Dedicated Link Policy
                    command aptpolicy completed

switch_A_1:admin> dlsshow
DLS is not set
```

> You must run these commands on both switches.

4. Verify that the ISLs are online and trunked (if the linking equipment supports trunking) using the **`islshow`** and **`trunkshow`** commands.

If FEC is enabled, the deskew value of the last online port of the trunk group might show a difference of up to 36 although the cables are all of the same length.

Are ISLs trunked?	You see the following system output…

Yes	If the ISLs are trunked, only a single ISL appears in the output for the **islshow** command. Either port 40 or 41 can appear depending on which is the trunk master. The output of **trunkshow** should one trunk with ID '1' listing both the physical ISLs on ports 40 and 41. In the following example the ports 40 and 41 are configured for use as an ISL:
	`switch_A_1:admin> islshow 1:`
	`40-> 40 10:00:00:05:33:88:9c:68 2`
	`switch_B_1 sp: 16.000G bw:`
	`32.000G TRUNK CR_RECOV FEC`
	`switch_A_1:admin> trunkshow`
	`1: 40-> 40`
	`10:00:00:05:33:88:9c:68 2 deskew`
	`51 MASTER`
	`41-> 41 10:00:00:05:33:88:9c:68 2`
	`deskew 15`

Are ISLs trunked?	You see the following system output…

No	If the ISLs are not trunked, both ISLs appear separately in the outputs for **`islshow`** and **`trunkshow`**. Both commands list the ISLs with their ID of '1' and '2'. In the following example, the ports 40 and 41 are configured for use as an ISL:
	`switch_A_1:admin> islshow`
	`1: 40-> 40`
	`10:00:00:05:33:88:9c:68 2`
	`switch_B_1 sp: 16.000G bw:`
	`16.000G TRUNK CR_RECOV FEC`
	`2: 41-> 41`
	`10:00:00:05:33:88:9c:68 2`
	`switch_B_1 sp: 16.000G bw:`
	`16.000G TRUNK CR_RECOV FEC`
	`switch_A_1:admin> trunkshow`
	`1: 40-> 40`
	`10:00:00:05:33:88:9c:68 2 deskew`
	`51 MASTER`
	`2: 41-> 41`
	`10:00:00:05:33:88:9c:68 2 deskew`
	`48 MASTER`

5. Run the **`spinfab`** command on both switches to verify that the ISLs are healthy:

```
switch_A_1:admin> spinfab -ports 0/40 - 0/41
```

6. Enable the ports that were disabled in step 1:

   `portenable port number`

   The following example shows ISL ports 0—7 being enabled:

```
brocade_switch_A_1:admin> portenable 0-7
```

Replacing a Cisco FC switch

You must use Cisco-specific steps to replace a failed Cisco FC switch.

You need the admin password and access to an FTP or SCP server.

This procedure is nondisruptive and takes approximately two hours to complete.

In the examples in this procedure, FC_switch_A_1 is the healthy switch and FC_switch_B_1 is the impaired switch. The switch port usage in the examples is shown in the following table:

Role	Ports
FC-VI connections	1, 4
HBA connections	2, 3, 5, 6
FC-to-SAS bridge connections	7, 8
ISL connections	36, 40

The examples show two FC-to-SAS bridges. If you have more, you must disable and subsequently enable the additional ports.

Your switch port usage should follow the recommended assignments.

- Port assignments for FC switches when using ONTAP 9.0
- Port assignments for FC switches when using ONTAP 9.1 and later

Steps

1. Disable the ISL ports on the healthy switch to fence off the impaired switch.

   These steps are performed on the healthy switch.

   a. Enter configuration mode:
      `conf t`

   b. Disable the ISL ports on the healthy switch with the `interface` and `shut` commands.

   ```
   FC_switch_A_1# conf t
   FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config)# shut
   FC_switch_A_1(config)# interface fc1/40
   FC_switch_A_1(config)# shut
   ```

   c. Exit configuration mode and copy the configuration to the startup configuration.

   ```
   FC_switch_A_1(config)# end
   FC_switch_A_1# copy running-config startup-config
   FC_switch_A_1#
   ```

2. Fence off the FC-VI and HBA ports on the impaired switch (if it is still running).

   These steps are performed on the impaired switch.

a. Enter configuration mode:
`conf t`

b. If the impaired switch is still operational, disable the FC-VI and HBA ports on the impaired switch with the interface and shut commands.

```
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
```

c. Exit configuration mode and copy the configuration to the startup configuration.

```
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

3. If the impaired switch is still operational, determine the WWN for the switch:

   `show wwn switch`

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:e3:86:50
FC_switch_B_1#
```

4. Boot and preconfigure the replacement switch, prior to physically installing it.

   At this point the replacement switch is not cabled to the MetroCluster configuration. The ISL ports on the partner switch are disabled (in shut mode) and offline.

   a. Power on the replacement switch and let it boot up.

   b. Check the firmware version on the replacement switch to confirm that it matches the version of the other FC switches:
   `show version`

   c. Configure the replacement switch as described in the *MetroCluster Installation and Configuration Guide*, skipping the “Configuring zoning on a Cisco FC switch” section.

   Fabric-attached MetroCluster installation and configuration

   You will configure zoning later in this procedure.

   d. Disable the FC-VI, HBA, and storage ports on the replacement switch.

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/1
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/4
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/2-3
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/5-6
FC_switch_B_1(config)# shut
FC_switch_B_1(config)# interface fc1/7-8
FC_switch_B_1(config)# shut
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

5. Physically replace the impaired switch:
   a. Power off the impaired switch.
   b. Power off the replacement switch.
   c. Uncable and remove the impaired switch, carefully noting which cables connected to which ports.
   d. Install the replacement switch in the rack.
   e. Cable the replacement switch exactly as the impaired switch was cabled.
   f. Power on the replacement switch.
6. Enable the ISL ports on the replacement switch.

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# interface fc1/36
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1(config)# interface fc1/40
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1#
```

7. Verify that the ISL ports on the replacement switch are up:

   `show interface brief`

8. Adjust the zoning on the replacement switch to match the MetroCluster configuration:

   a. Distribute the zoning information from the healthy fabric.

      In this example, FC_switch_B_1 has been replaced and the zoning information is retrieved from FC_switch_A_1:

```
FC_switch_A_1(config-zone)# zoneset distribute full vsan 10
FC_switch_A_1(config-zone)# zoneset distribute full vsan 20
FC_switch_A_1(config-zone)# end
```

b. On the replacement switch, verify that the zoning information was properly retrieved from the healthy switch:
`show zone`

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/4 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/4 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/3 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/6 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/3 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/6 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

c. Find the WWNs of the switches.

In this example, the two switch WWNs are as follows:

- FC_switch_A_1: 20:00:54:7f:ee:b8:24:c0
- FC_switch_B_1: 20:00:54:7f:ee:c6:80:78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

d. Remove zone members that do not belong to the switch WWNs of the two switches.

   In this example, `no member interface` in the output shows that the following members are not associated with the switch WWN of either of the switches in the fabric and must be removed:

   - zone name FC-VI_Zone_1_10 vsan 10
     - interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
     - interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
   - zone name STOR_Zone_1_20_25A vsan 20
     - interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
     - interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
     - interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
     - interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
     - interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
   - zone name STOR_Zone_1_20_25B vsan 20
     - interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
     - interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
     - interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
     - interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50 The following example shows the removal of these interfaces:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

a. Add the ports of the replacement switch to the zones.

   All the cabling on the replacement switch must be the same as on the impaired switch:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

b. Verify that the zoning is properly configured:
`show zone`

The following example output shows the three zones:

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

c. Enable the connectivity to storage and the controllers.

   The following example shows the port usage:

```
FC_switch_A_1# conf t
FC_switch_A_1(config)# interface fc1/1
FC_switch_A_1(config)# no shut
FC_switch_A_1(config)# interface fc1/4
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/2-3
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/5-6
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# interface fc1/7-8
FC_switch_A_1(config)# shut
FC_switch_A_1# copy running-config startup-config
FC_switch_A_1#
```

9. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:
      `node run -node` ***`node-name`*** **`sysconfig -a`**
   b. Check for any health alerts on both clusters:
      `system health alert show`
   c. Confirm the MetroCluster configuration and that the operational mode is normal:

      `metrocluster show`

   d. Perform a MetroCluster check:

      `metrocluster check run`

   e. Display the results of the MetroCluster check:
      `metrocluster check show`
   f. Check for any health alerts on the switches (if present):
      `storage switch show`
   g. Run Config Advisor.

      NetApp Downloads: Config Advisor

   h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Changing speed of ISL ports on a Cisco FC switch

You might need to change the speed of ISL ports on a switch to improve the quality of the ISL. ISLs traveling greater distances might need their speed lowered to improve quality.

You must complete all the steps on both switches to ensure ISL connectivity.

1. Disable the ISL ports of the ISLs that you want to change the speed of on both switches in the fabric:

FC_switch_A_1# config t

Enter configuration commands, one per line. End with CTRL-Z after you have entered all of the configuration commands.

```
FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# shut
   FC_switch_A_1(config)# end
```

2. Change the speed of the ISL ports on both switches in the fabric:

   FC_switch_A_1# config t

   Enter configuration commands, one per line. End with CTRL-Z after you have entered all of the configuration commands.

```
FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# switchport speed 16000
```

> Speeds for ports are 16 = 16,000 Gbps, 8 = 8,000 Gbps, 4 = 4,000 Gbps.

   Ensure that these ISL ports for your switch are listed in the *Fabric-attached MetroCluster Installation and Configuration Guide*.

3. Enable all ISL ports (if not enabled) on both switches in the fabric:

   FC_switch_A_1# config t

   Enter configuration commands, one per line. End with CTRL-Z after you have entered all of the configuration commands.

```
FC_switch_A_1(config)# interface fc1/36
   FC_switch_A_1(config-if)# no shut
   FC_switch_A_1(config)# end
```

4. Verify the ISLs are established between both switches:

   show topology isl

```
--------------------------------------------------------------------------------
--------
    __________Local_________ _________Remote_________ VSAN Cost I/F  PC
I/F  Band
     PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
Speed width

--------------------------------------------------------------------------------
--------
      1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
16g   64g
```

5. Repeat the procedure for the second switch fabric.

Adding ISLs to a Cisco switch

You might need to add ISLs to a switch if you are adding or upgrading hardware such as additional or faster controllers or faster switches.

Steps that are completed on one switch must also be completed on the other to ensure ISL connectivity.

Steps

1. Disable the ISL ports of the ISLs to be added on both switches in the fabric:

   `FC_switch_A_1#config t`

   Enter the configuration commands, one per line. End with CTRL-Z after all the configuration commands have been entered.

   ```
       FC_switch_A_1(config)# interface fc1/36
       FC_switch_A_1(config-if)# shut
       FC_switch_A_1(config)# end
   ```

2. Insert SFPs into the ports you are adding as ISL ports, and cable them according to the *Installation and Configuration Guide*.

   Ensure that these ports are listed in the *Installation and Configuration Guide* for the switch you are adding them to.

3. Configure the ISL ports in accordance with the *Installation and Configuration Guide*.

4. Enable all ISL ports (if not enabled) on both switches in the fabric:

   `FC_switch_A_1# config t`

   Enter the configuration commands, one per line. End with CTRL-Z.

```
 FC_switch_A_1# interface fc1/36
    FC_switch_A_1(config-if)# no shut
    FC_switch_A_1(config)# end
```

5. Verify the ISLs are established between both switches:

   `show topology isl`

6. Repeat the procedure on the second fabric:

```
--------------------------------------------------------------------------------
--------
    __________Local_________ _________Remote_________ VSAN Cost I/F  PC
I/F  Band
     PC Domain SwName   Port  Port   SwName Domain PC          Stat Stat
Speed width

--------------------------------------------------------------------------------
--------
      1   0x11 cisco9 fc1/36  fc1/36 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/40  fc1/40 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/44  fc1/44 cisco9 0xbc    1    1   15 up   up
16g   64g
      1   0x11 cisco9 fc1/48  fc1/48 cisco9 0xbc    1    1   15 up   up
16g   64g
```

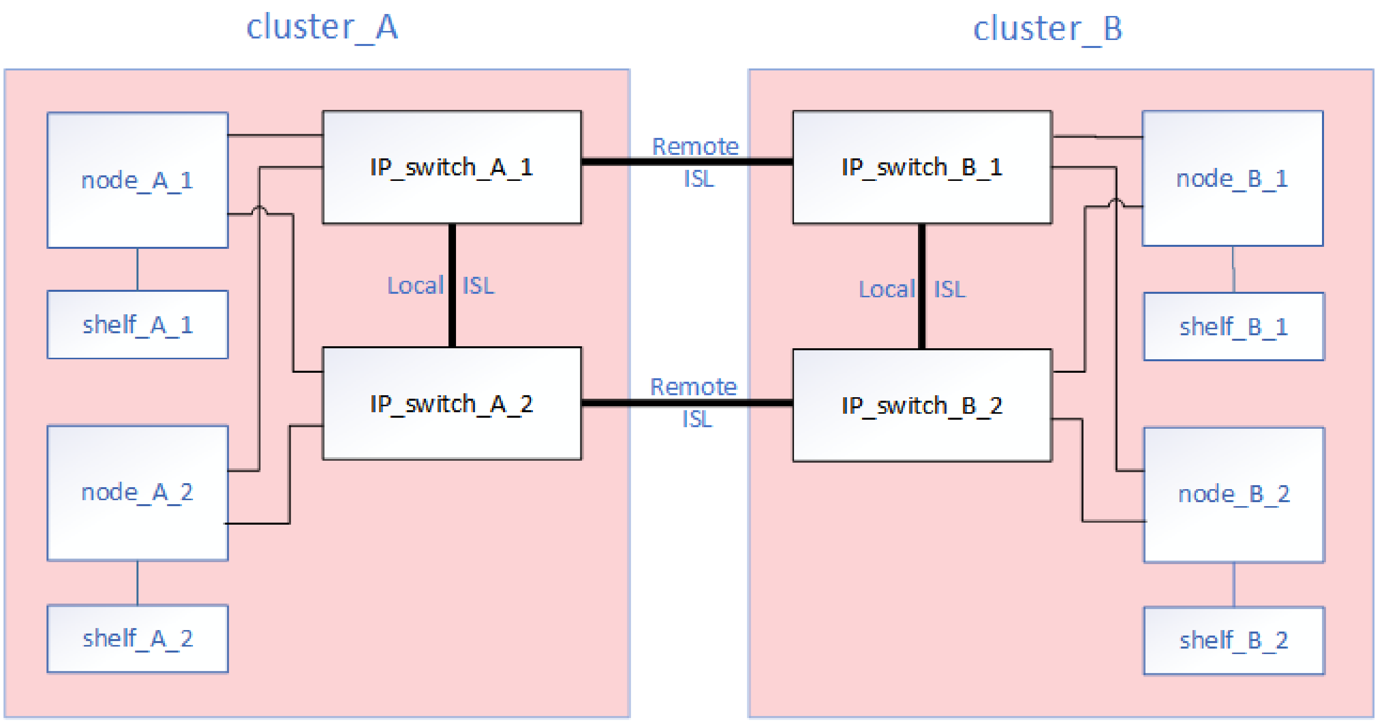
Performing IP switch maintenance and replacement

If necessary, you can nondisruptively upgrade, downgrade, or replace the IP switches in a MetroCluster configuration.

Replacing an IP switch

You might need to replace a failed switch, or upgrade or downgrade a switch. The new switch can be the same as the old switch when a switch has failed, or you can change the switch type (upgrade or downgrade the switch).

If you want to replace a failed switch with the same type of switch, you only need to replace the failed switch. If you want to upgrade or downgrade a switch, you need to adjust two switches that are in the same network. Two switches are in the same network if they are connected with an inter-switch link (ISL) and are not located at the same site. For example, Network 1 includes IP_switch_A_1 and IP_switch_B_1. Network 2 includes IP_switch_A_2 and IP_switch_B_2 as shown in the diagram below:



This procedure is for Cisco or Broadcom switches. If you want to change the switch vendor, further steps are required.

If you upgrade or downgrade the networks, you must repeat this procedure for the second network.

Steps

1. Check the health of the configuration.

   a. Check that the MetroCluster is configured and in normal mode on each cluster: **`metrocluster show`**

```
cluster_A::> metrocluster show
Cluster                    Entry Name          State
-------------------------- ------------------- -----------
 Local: cluster_A          Configuration state configured
                           Mode                normal
                           AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B          Configuration state configured
                           Mode                normal
                           AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Check that mirroring is enabled on each node: **`metrocluster node show`**

```
cluster_A::> metrocluster node show
DR                                Configuration   DR
Group Cluster Node                State           Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1        configured      enabled   normal
      cluster_B
              node_B_1        configured      enabled   normal
2 entries were displayed.
```

c. Check that the MetroCluster components are healthy: **`metrocluster check run`**

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. Check that there are no health alerts: **`system health alert show`**

2. Configure the new switch before installation.

   > If you are upgrading or downgrading the switches, you must configure all the switches in the network.

   Follow the steps in the section *Configuring the IP switches* in the [MetroCluster IP Installation and Configuration Guide.]

   Make sure that you apply the correct RCF file for switch _A_1, _A_2, _B_1 or _B_2. If the new switch is the same as the old switch, you need to apply the same RCF file.

   If you upgrade or downgrade a switch, apply the latest supported RCF file for the new switch.

3. Run the port show command to view information about the network ports:

   `network port show`

4. Disconnect the ISL connections from the remote switch that connect to the old switch.

   You should disconnect the ISL connections from the ports on the IP_switch_A_1 that connect to IP_switch_B_1.

5. Power off the switch, remove the cables and physically remove IP_switch_B_1.
6. Install the new switch.

   Cable the new switch first (including the ISLs) according to the steps in the *Cabling the IP switches* section in the MetroCluster IP Installation and Configuration Guide.

   > The used ports might be different from those on the old switch if the switch type is different. If you are upgrading or downgrading the switches, do **NOT** cable the local ISLs. Only cable the local ISLs if you are upgrading or downgrading the switches in the second network and both switches at one site are the same type.

7. Power up the switch or switches.

   If the new switch is the same, power up the new switch. If you are upgrading or downgrading the switches, then power up both switches. The configuration can operate with two different switches at each site until the second network is updated.

8. Verify that the MetroCluster configuration is healthy by repeating step 1.

   If you are upgrading or downgrading the switches in the first network, you might see some alerts related to local clustering.

   > If you upgrade or downgrade the networks, then repeat all of the steps for the second network.

Upgrading firmware on MetroCluster IP switches

You might need to upgrade the firmware on a MetroCluster IP switch.

When you install the switch software on each of the switch, you must first check the health of the configuration.

You must repeat this task on each of the switch in succession to ensure that all MetroCluster components are healthy.

Steps

1. Check the health of the configuration.
   a. Check that the MetroCluster is configured and in normal mode on each cluster: **`metrocluster show`**

```
cluster_A::> metrocluster show
Cluster                    Entry Name          State
-------------------------- ------------------- -----------
 Local: cluster_A          Configuration state configured
                           Mode                normal
                           AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B          Configuration state configured
                           Mode                normal
                           AUSO Failure Domain auso-on-cluster-
disaster
```

b. Check that mirroring is enabled on each node: **`metrocluster node show`**

```
cluster_A::> metrocluster node show
DR                            Configuration  DR
Group Cluster Node            State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1       configured     enabled   normal
      cluster_B
              node_B_1       configured     enabled   normal
2 entries were displayed.
```

c. Check that the MetroCluster components are healthy: **`metrocluster check run`**

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

d. Check that there are no health alerts: **`system health alert show`**

2. Install the software on the first switch.

   Follow the steps for installing switch software in the relevant section in the *MetroCluster IP Installation and Configuration Guide* depending on whether the switch type is Cisco or Broadcom:

   MetroCluster IP Installation and Configuration Guide

3. Repeat the previous step for each of the switches.
4. Repeat step 1 to check the health of the configuration.

Upgrading RCF files on MetroCluster IP switches

You might need to upgrade an RCF file on a MetroCluster IP switch. For example, an ONTAP upgrade or a switch firmware upgrade both require a new RCF file.

If you are installing new switch firmware, you must install the switch firmware before upgrading the RCF file.

This procedure disrupts traffic on the switch where the RCF file is upgraded. Traffic will resume once the new RCF file is applied.

Steps

1. Verify the health of the configuration.

   a. Verify that the MetroCluster components are healthy:

      `metrocluster check run`

```
cluster_A::*> metrocluster check run
```

The operation runs in the background.

a. After the `metrocluster check run` operation completes, run `metrocluster check show` to view the results.

   After approximately five minutes, the following results are displayed:

```
-----------
::*> metrocluster check show

Last Checked On: 4/7/2019 21:15:05

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          warning
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

b. To check the status of the running MetroCluster check operation, use the command:
   `metrocluster operation history show -job-id 38`

c. Verify that there are no health alerts:
   `system health alert show`

2. Prepare the IP switches for the application of the new RCF files.

   Follow the steps in the section for your switch vendor from the *MetroCluster IP Installation and Configuration guide*.

   MetroCluster IP installation and configuration

   - *Resetting the Broadcom IP switch to factory defaults*
   - *Resetting the Cisco IP switch to factory defaults*

3. Download and install the IP RCF file depending on your switch vendor.

   Follow the steps in the section for your switch vendor from the *MetroCluster IP Installation and Configuration guide*.

   MetroCluster IP installation and configuration

   - *Downloading and installing the Broadcom IP RCF files*

◦ *Downloading and installing the Cisco IP RCF files*

a. Update the switches in the following order: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.

Renaming a Cisco IP switch

You might need to rename a Cisco IP switch to provide consistent naming throughout your configuration.

In the examples in this task, the switch name is changed from `myswitch` to `IP_switch_A_1`.

1. Enter global configuration mode:

   `configure terminal`

   The following example shows the configuration mode prompt. Both prompts show the switch name of `myswitch`.

   ```
   myswitch# configure terminal
   myswitch(config)#
   ```

2. Rename the switch:

   `switchname new-switch-name`

   If you are renaming both switches in the fabric, use the same command on each switch.

   The CLI prompt changes to reflect the new name:

   ```
   myswitch(config)# switchname IP_switch_A_1
   IP_switch_A_1(config)#
   ```

3. Exit configuration mode:

   `exit`

   The top-level switch prompt is displayed:

   ```
   IP_switch_A_1(config)# exit
   IP_switch_A_1#
   ```

4. Copy the current running configuration to the startup configuration file:

   `copy running-config startup-config`

5. Verify that the switch name change is visible from the ONTAP cluster prompt.

   Note that the new switch name is shown, and the old switch name (`myswitch`) does not appear.

a. Enter advanced privilege mode, pressing **y** when prompted:
set -privilege advanced

b. Display the attached devices:
network device-discovery show

c. Return to admin privilege mode:
set -privilege admin

The following example shows that the switch appears with the new name, `IP_switch_A_1`:

```
cluster_A::storage show> set advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

cluster_A::storage show*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device                    Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node_A_2/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/28  N9K-
C9372PX
            e1a    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/2       N3K-
C3232C
            e1b    IP_switch_A_1(FOC21211RBU)
                                             Ethernet1/10      N3K-
C3232C
.
.
.                                             Ethernet1/18      N9K-
C9372PX
node_A_1/cdp
            e0M    LF01-410J53.mycompany.com(SAL18516DZY)
                                             Ethernet125/1/26  N9K-
C9372PX
            e0a    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/1       N3K-
C3232C
            e0b    IP_switch_A_2(FOC21211RB5)
                                             Ethernet1/9       N3K-
C3232C
            e1a    IP_switch_A_1(FOC21211RBU)
.
.
.
16 entries were displayed.
```

Adding, removing, or changing ISL ports nondisruptively

You might need to add, remove, or change ISL ports. You can convert dedicated ISL ports to shared ISL ports, or change the speed of ISL ports on a switch. ISLs traveling greater distances might require lower speeds to improve quality. You also might need to increase the speed of ISL ports to take advantage of system upgrades and add ISLs to a Cisco IP switch if you are adding or upgrading hardware.

If you are converting dedicated ISL ports to shared ISL ports, ensure the new ports meet the requirements for shared ISL ports.

You must complete all the steps on both switches to ensure ISL connectivity.

The following procedure assumes you are replacing a 10-Gb ISL connected at switch port Eth1/24/1 with two 100-Gb ISLs that are connected to switch ports 17 and 18.

Steps

1. Disable the ISL ports of the ISLs on both switches in the fabric that you want to change.

   > You only need to disable the current ISL ports if you are moving them to a different port, or the speed of the ISL is changing. If you are adding an ISL port with the same speed as the existing ISLs, go to Step 3.

   You must enter only one configuration command for each line and press Ctrl-Z after you have entered all the commands, as shown in the following example:

   ```
   switch_A_1# conf t
   switch_A_1(config)# int eth1/24/1
   switch_A_1(config-if)# shut
   switch_A_1(config-if)#
   switch_A_1#

   switch_B_1# conf t
   switch_B_1(config)# int eth1/24/1
   switch_B_1(config-if)# shut
   switch_B_1(config-if)#
   switch_B_1#
   ```

2. Remove the existing cables and transceivers.
3. Change the ISL port as required.

Option	Step
To change the speed of an ISL port…	Cable the new ISLs to the designated ports according to their speeds. You must ensure that these ISL ports for your switch are listed in the *MetroCluster IP Installation and Configuration Guide*.
To add an ISL…	Insert QFSPs into the ports you are adding as ISL ports. Ensure they are listed in the *MetroCluster IP Installation and Configuration Guide* and cable them according to this guide.

4. Enable all ISL ports (if not enabled) on both switches in the fabric beginning with the following command:

   `switch_A_1# conf t`

   You must enter only one configuration command per line and press Ctrl-Z after you have entered all the commands:

```
switch_A_1# conf t
switch_A_1(config)# int eth1/17
switch_A_1(config-if)# no shut
switch_A_1(config-if)# int eth1/18
switch_A_1(config-if)# no shut
switch_A_1(config-if)#
switch_A_1#
switch_A_1# copy running-config startup-config

switch_B_1# conf t
switch_B_1(config)# int eth1/17
switch_B_1(config-if)# no shut
switch_B_1(config-if)# int eth1/18
switch_B_1(config-if)# no shut
switch_B_1(config-if)#
switch_B_1#
switch_B_1# copy running-config startup-config
```

5. Verify that the ISLs are established between both switches:

   `switch_A_1# show int eth1/17,eth1/18 brief`

   You should see the ISL interfaces in the command output as shown in the following example:

```
switch_A_1# show int eth1/17,eth1/18 brief
--------------------------------------------------------------------------
--------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed
Port
Interface
Ch #
--------------------------------------------------------------------------
--------
Eth1/17       10         eth     access    up      none
100G(D) 10
Eth1/18       10         eth     access    up      none
100G(D) 10

switch_B_1# show int eth1/17,eth1/18 brief
--------------------------------------------------------------------------
--------
Ethernet      VLAN    Type Mode   Status  Reason                   Speed
Port
Interface
Ch #
--------------------------------------------------------------------------
--------
Eth1/17       10         eth     access    up      none
100G(D) 10
Eth1/18       10         eth     access    up      none
100G(D) 10
```

6. Repeat the procedure for fabric 2.

Identifying storage in a MetroCluster IP configuration

If you need to replace a drive or shelf module, you first need to identify the location.

Identification of local and remote shelves

When you view shelf information from a MetroCluster site, all remote drives are on 0m, the virtual iSCSI host adapter. This means that the drives are accessed via the MetroCluster IP interfaces. All other drives are local.

After identifying whether a shelf is remote (on 0m), you can further identify the drive or shelf by the serial number or, depending on shelf ID assignments in your configuration, by shelf ID.

> In MetroCluster IP configurations running ONTAP 9.4, the shelf ID is not required to be unique between the MetroCluster sites. This includes both internal shelves (0) and external shelves. The serial number is consistent when viewed from any node on either MetroCluster site.

Shelf IDs should be unique within the disaster recovery (DR) group except for the internal shelf.

With the drive or shelf module identified, you can replace the component using the appropriate procedure.

Service Guide for DS460C DS224C and DS212C Disk Shelves

Example of sysconfig -a output

The following example uses the `sysconfig -a` command to show the devices on a node in the MetroCluster IP configuration. This node has the following shelves and devices attached:

- slot 0: Internal drives (local drives)
- slot 3: External shelf ID 75 and 76 (local drives)
- slot 0: Virtual iSCSI host adapter 0m (remote drives)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
                0    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
                1    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
                2    : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:80
Phy State:          [12] Enabled, 12.0 Gb/s
                    [13] Enabled, 12.0 Gb/s
                    [14] Enabled, 12.0 Gb/s
                    [15] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
```

```
Mini-SAS HD Serial Number: 614130640
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
                75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                    [1] Enabled, 12.0 Gb/s
                    [2] Enabled, 12.0 Gb/s
                    [3] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
```

```
slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:    Microsemi Corp. 110-03801 rev. A0
Part number:        111-03801+A0
Serial number:      7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:8c
Phy State:          [4] Enabled, 12.0 Gb/s
                    [5] Enabled, 12.0 Gb/s
                    [6] Enabled, 12.0 Gb/s
                    [7] Enabled, 12.0 Gb/s
Mini-SAS HD Vendor:        Molex Inc.
Mini-SAS HD Part Number:   112-00436+A0
Mini-SAS HD Type:          Passive Copper (unequalized) 0.5m ID:01
Mini-SAS HD Serial Number: 614130690
                75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
.
.
.
Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+
.
.
.
slot 0: Virtual iSCSI Host Adapter 0m
                0.0  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)
                0.1  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)
                0.2  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)
                0.3  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500724)
                0.4  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
                0.5  : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500598)
                0.12 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
```

```
(S3NBNX0J501094)
                0.13 : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E  Firmware rev. PSM3E A: 0103  PSM3E B: 0103
Shelf 35: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 36: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

node_A_1::>
```

Hot-adding storage to a MetroCluster FC configuration

You can add storage to a MetroCluster FC configuration without bringing down the system. The procedure you use depends on the type of MetroCluster FC configuration and whether you are adding a single disk shelf to an existing stack or an entire stack.

Hot-adding a SAS disk shelf in a direct-attached MetroCluster FC configuration using SAS optical cables

You can use SAS optical cables to hot-add a SAS disk shelf to an existing stack of SAS disk shelves in a direct-attached MetroCluster FC configuration, or as a new stack to a SAS HBA or an onboard SAS port on the controller.

- This procedure is nondisruptive and takes approximately two hours to complete.
- You need the admin password and access to an FTP or SCP server.
- If you are adding an IOM12 shelf to a stack of IOM6 shelves, see Hot-adding IOM12 shelves to a stack of IOM6 shelves.

This task applies to a MetroCluster FC configuration in which the storage is connected directly to the storage controllers with SAS cables. It does not apply to MetroCluster FC configurations using FC-to-SAS bridges or FC switch fabrics.

Steps

1. Follow the instructions for hot-adding a SAS disk shelf in the *Installation Guide* for your disk shelf model to perform the following tasks to hot-add a disk shelf:
   a. Install a disk shelf for a hot-add.
   b. Turn on the power supplies and set the shelf ID for a hot-add.
   c. Cable the hot-added disk shelf.
   d. Verify SAS connectivity.

Hot-adding SAS storage to a bridge-attached MetroCluster FC configuration

You can hot-add either an individual SAS disk shelf or a stack and set of bridges to an existing MetroCluster system.

These procedures apply to MetroCluster FC configurations using FC-to-SAS bridges that are either directly attached to the storage controllers or attached to an FC fabric.

These procedures are nondisruptive and take approximately four hours to complete.

You need the admin password and access to an FTP or SCP server.

Hot-adding a stack of SAS disk shelves to an existing pair of FibreBridge 7500N bridges

You can hot-add a stack of SAS disk shelves to an existing pair of FibreBridge 7500N bridges that have available ports.

- You must have downloaded the latest disk and disk shelf firmware.
- All of the disk shelves in the MetroCluster configuration (both the new shelves and existing shelves) must be running the same firmware version.

  NetApp Downloads: Disk Drive Firmware

  NetApp Downloads: Disk Shelf Firmware
- The FibreBridge 7500N bridges must be connected and have available SAS ports.

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

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

You can use other management interfaces, if required. These options include using a serial port or Telnet to configure and manage a bridge and to configure the Ethernet management 1 port, and using FTP to update the bridge firmware. If you choose any of these management interfaces, you must meet the applicable requirements in Other bridge management interfaces.

> If you insert a SAS cable into the wrong port, when you remove the cable from a SAS port, you must wait at least 120 seconds before plugging the cable into a different SAS port. If you fail to do so, the system will not recognize that the cable has been moved to another port.

Steps

1. Properly ground yourself.
2. From the console of either controller, verify that your system has disk autoassignment enabled:

   `storage disk option show`

   The Auto Assign column indicates whether disk autoassignment is enabled.

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on          on           on           default
   node_A_2             on          on           on           default
   2 entries were displayed.
   ```

3. Disable the switch ports for the new stack.
4. Update the FibreBridge firmware on each bridge.

   If the new bridge is the same type as the partner bridge upgrade to the same firmware as the partner bridge. If the new bridge is a different type to the partner bridge, upgrade to the latest firmware supported by the bridge and version of ONTAP. See the section "Updating firmware on a FibreBridge bridge" in the *MetroCluster Maintenance Guide*.

5. On each bridge in the pair, enable the SAS port that will connect to the new stack:

   `SASPortEnable` ***`port-letter`***

   The same SAS port (B, C, or D) must be used on both bridges.

6. Save the configuration and reboot each bridge:

   `SaveConfiguration Restart`

7. Cable the disk shelves to the bridges:
   a. Daisy-chain the disk shelves in each stack.

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

   b. For each stack of disk shelves, cable IOM A of the first shelf to SAS port A on FibreBridge A, and then cable IOM B of the last shelf to SAS port A on FibreBridge B

      Fabric-attached MetroCluster installation and configuration

      Stretch MetroCluster installation and configuration

      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.

      > The bridge SAS port B is disabled.

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

If you are using the…	Then…
ATTO ExpressNAV GUI	a. In a supported web browser, enter the IP address of a bridge in the browser box. You are brought to the ATTO FibreBridge home page, which has a link. 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 appears with a menu to the left. c. Click **Advanced** in the menu. d. View the connected devices: **`sastargets`** e. Click **Submit**.
Serial port connection	View the connected devices: **`sastargets`**

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

> If the text `response truncated` appears at the beginning of the output, you can use Telnet to connect to the bridge, and then view all of the output by using the `sastargets` command.

The following output shows that 10 disks are connected:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

9. Verify that the command output shows that the bridge is connected to all of the appropriate disks and disk shelves in the stack.

If the output is…	Then…
Correct	Repeat the previous step for each remaining bridge.
Not correct	a. Check for loose SAS cables or correct the SAS cabling by repeating the step to cable the disk shelves to the bridges. b. Repeat the previous step for each remaining bridge.

10. Cable each bridge to the local FC switches, using the cabling shown in the table for your configuration, switch model, and FC-to-SAS bridge model:

> The Brocade and Cisco switches use different port numbering, as shown in the following tables
>
> ◦ On Brocade switches, the first port is numbered “0”.
>
> ◦ On Cisco switches, the first port is numbered “1”.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)												
DR GROUP 1												
			Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Component		Port	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2
Stack 1	bridge _x_1a	FC1	8		8		8		8		10	
		FC2	-	8	-	8	-	8	-	8	-	10
	bridge _x_1B	FC1	9	-	9	-	9	-	9	-	11	-
		FC2	-	9	-	9	-	9	-	9	-	11
Stack 2	bridge _x_2a	FC1	10	-	10	-	10	-	10	-	14	-
		FC2	-	10	-	10	-	10	-	10	-	14
	bridge _x_2B	FC1	11	-	11	-	11	-	11	-	17	-
		FC2	-	11	-	11	-	11	-	11	-	17

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)												
Stack 3	bridge _x_3a	FC1	12	-	12	-	12	-	12	-	18	-
		FC2	-	12	-	12	-	12	-	12	-	18
	bridge _x_3B	FC1	13	-	13	-	13	-	13	-	19	-
		FC2	-	13	-	13	-	13	-	13	-	19
Stack y	bridge _x_ya	FC1	14	-	14	-	14	-	14	-	20	-
		FC2	-	14	-	14	-	14	-	14	-	20
	bridge _x_yb	FC1	15	-	15	-	15	-	15	-	21	-
		FC2		15		15		15	-	15	-	21

ⓘ Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620, G630, G620-1, and G630-1 switches.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)										
DR GROUP 2										
			Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G720	
Component		Port	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	switch 2
Stack 1	bridge_x_51a	FC1	26	-	32	-	56	-	32	-
		FC2	-	26	-	32	-	56	-	32
	bridge_x_51b	FC1	27	-	33	-	57	-	33	-
		FC2	-	27	-	33	-	57	-	33
Stack 2	bridge_x_52a	FC1	30	-	34	-	58	-	34	-
		FC2	-	30	-	34	-	58	-	34
	bridge_x_52b	FC1	31	-	35	-	59	-	35	-
		FC2	-	31	-	35	-	59	-	35

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)										
Stack 3	bridge_ x_53a	FC1	32	-	36	-	60	-	36	-
		FC2	-	32	-	36	-	60	-	36
	bridge_ x_53b	FC1	33	-	37	-	61	-	37	-
		FC2	-	33	-	37	-	61	-	37
Stack y	bridge_ x_5ya	FC1	34	-	38	-	62	-	38	-
		FC2	-	34	-	38	-	62	-	38
	bridge_ x_5yb	FC1	35	-	39	-	63	-	39	-
		FC2	-	35	-	39	-	63	-	39

Additional bridges can be cabled to ports 36 - 39 in G620, G630, G620-1, and G-630-1 switches.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only											
DR GROUP 1											
		Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Component	Port	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2
Stack 1	bridge_ x_1a	8		8		8		8		10	
	bridge_ x_1b	-	8	-	8	-	8	-	8	-	10
Stack 2	bridge_ x_2a	9	-	9	-	9	-	9	-	11	-
	bridge_ x_2b	-	9	-	9	-	9	-	9	-	11

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only											
Stack 3	bridge_x_3a	10	-	10	-	10	-	10	-	14	-
	bridge_x_4b	-	10	-	10	-	10	-	10	-	14
Stack y	bridge_x_ya	11	-	11	-	11	-	11	-	15	-
	bridge_x_yb	-	11	-	11	-	11	-	11	-	15

Additional bridges can be cabled to ports 12 - 17, 20 and 21 in G620, G630, G620-1, and G630-1 switches. Additional bridges can be cabled to ports 16 - 17, 20 and 21 G720 switches.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only									
DR GROUP 2									
		Brocade G720		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520	
Stack 1	bridge_x_51a	32	-	26	-	32	-	56	-
	bridge_x_51b	-	32	-	26	-	32	-	56
Stack 2	bridge_x_52a	33	-	27	-	33	-	57	-
	bridge_x_52b	-	33	-	27	-	33	-	57
Stack 3	bridge_x_53a	34	-	30	-	34	-	58	-
	bridge_x_54b	-	34	-	30	-	34	-	58

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only									
Stack y	bridge_x_ya	35	-	31	-	35	-	59	-
	bridge_x_yb	-	35	-	31	-	35	-	59

> Additional bridges can be cabled to ports 32 - 39 in G620, G630, G620-1, and G630-1 switches. Additional bridges can be cabled to ports 36 - 39 in G720 switches.

11. Update the disk drive firmware to the most current version from the system console:

    `disk_fw_update`

    You must run this command on both controllers.

    NetApp Downloads: Disk Drive Firmware

12. Update the disk shelf firmware to the most current version by using the instructions for the downloaded firmware.

    You can run the commands in the procedure from the system console of either controller.

    NetApp Downloads: Disk Shelf Firmware

13. If your system does not have disk autoassignment enabled, assign disk drive ownership.

    Disk and aggregate management

    > If you are splitting the ownership of a single stack of disk shelves among multiple controllers, you must disable disk autoassignment (`storage disk option modify -autoassign off *` from both nodes in the cluster) before assigning disk ownership; otherwise, when you assign any single disk drive, the remaining disk drives might be automatically assigned to the same controller and pool.

    > You must not add disk drives to aggregates or volumes until after the disk drive firmware and disk shelf firmware have been updated and the verification steps in this task have been completed.

14. Enable the switch ports for the new stack.
15. Verify the operation of the MetroCluster configuration in ONTAP:
    a. Check whether the system is multipathed:

       `node run -node` *`node-name`* `sysconfig -a`

    b. Check for any health alerts on both clusters:

       `system health alert show`

c. Confirm the MetroCluster configuration and that the operational mode is normal:

   `metrocluster show`

d. Perform a MetroCluster check:

   `metrocluster check run`

e. Display the results of the MetroCluster check:

   `metrocluster check show`

f. Check for any health alerts on the switches (if present):

   `storage switch show`

g. Run Config Advisor.

   NetApp Downloads: Config Advisor

h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

16. If applicable, repeat this procedure for the partner site.

Hot-adding a stack of SAS disk shelves and bridges to a MetroCluster system

You can hot-add (nondisruptively add) an entire stack, including the bridges, to the MetroCluster system. There must be available ports on the FC switches and you must update switch zoning to reflect the changes.

- This procedure can be used to add a stack using either FibreBridge 7500N or 6500N bridges.
- This procedure is written with the assumption that you are using the recommended bridge management interfaces: the ATTO ExpressNAV GUI and the 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, if needed. These options include using a serial port or Telnet to configure and manage a bridge, and to configure the Ethernet management 1 port, and using FTP to update the bridge firmware. If you choose any of these management interfaces, your system must meet the applicable requirements in Other bridge management interfaces

Preparing to hot-add a stack of SAS disk shelves and bridges

Preparing to hot-add a stack of SAS disk shelves and a pair of bridges involves downloading documents as well as the disk drive and disk shelf firmware.

- Your system must be a supported configuration and must be running a supported version of ONTAP.

  NetApp Interoperability Matrix Tool

- All disk drives and disk shelves in the system must be running the latest firmware version.

  You might want to update the disk and shelf firmware throughout the MetroCluster configuration prior to adding shelves.

Upgrade, revert, or downgrade

- Each FC switch must have one FC port available for one bridge to connect to it.

  You might need to upgrade the FC switch depending on the FC switch compatibility.

- The computer you are using to set up the bridges must be running an ATTO supported web browser to use the ATTO ExpressNAV GUI: Internet Explorer 8 or 9, or Mozilla Firefox 3.

  The *ATTO Product Release Notes* have an up-to-date list of supported web browsers. You can access this document using the information in the steps.

Steps

1. Download or view the following documents from the NetApp Support Site:
   - NetApp Interoperability Matrix Tool
   - The *Installation and Service Guide* for your disk shelf model.
2. Download content from the ATTO website and from the NetApp website:
   a. Go to the ATTO FibreBridge Description page.
   b. Using the link on the ATTO FibreBridge Description page, access the ATTO web site and download the following:
      - *ATTO FibreBridge Installation and Operation Manual* for your bridge model.
      - ATTO QuickNAV utility (to the computer you are using for setup).
   c. Go to the ATTO FibreBridge Firmware Download page by clicking **Continue** at the end of the ATTO FibreBridge Description page, and then do the following:
      - Download the bridge firmware file as directed on the download page.

        In this step, you are only completing the download portion of the instructions provided in the links. You update the firmware on each bridge later, when instructed to do so in the Hot-adding the stack of shelves section.
      - Make a copy of the ATTO FibreBridge Firmware Download page and release notes for reference later.
3. Download the latest disk and disk shelf firmware, and make a copy of the installation portion of the instructions for reference later.

   All disk shelves in the MetroCluster configuration (both the new shelves and existing shelves) must be running the same firmware version.

   In this step, you are only completing the download portion of the instructions provided in the links and making a copy of the installation instructions. You update the firmware on each disk and disk shelf later, when instructed to do so in the Hot-adding the stack of shelves section.

   a. Download the disk firmware and make a copy of the disk firmware instructions for reference later.

      NetApp Downloads: Disk Drive Firmware

b. Download the disk shelf firmware and make a copy of the disk shelf firmware instructions for reference later.

NetApp Downloads: Disk Shelf Firmware

4. Gather the hardware and information needed to use the recommended bridge management interfaces—the ATTO ExpressNAV GUI and ATTO QuickNAV utility:
   a. Acquire a standard Ethernet cable to connect from the bridge Ethernet management 1 port to your network.
   b. Determine a non-default user name and password for accessing the bridges.

      It is recommended that you change the default user name and password.

   c. Obtain 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.

5. Acquire four screws for each bridge to flush-mount the bridge “L” brackets securely to the front of the rack.

   The openings in the bridge “L” brackets are compliant with rack standard ETA-310-X for 19-inch (482.6 mm) racks.

6. If necessary, update the FC switch zoning to accommodate the new bridges that are being added to the configuration.

   If you are using the Reference Configuration Files provided by NetApp, the zones have been created for all ports, so you do not need to make any zoning updates. There must be a storage zone for each switch port that connects to the FC ports of the bridge.

Hot-adding a stack of SAS disk shelves and bridges

You can hot-add a stack of SAS disk shelves and bridges to increase the capacity of the bridges.

The system must meet all of the requirements to hot-add a stack of SAS disk shelves and bridges.

Preparing to hot-add a stack of SAS disk shelves and bridges

- Hot-adding a stack of SAS disk shelves and bridges is a nondisruptive procedure if all of the interoperability requirements are met.

  NetApp Interoperability Matrix Tool

  Using the Interoperability Matrix Tool to find MetroCluster information

- Multipath HA is the only supported configuration for MetroCluster systems that are using bridges.

  Both controller modules must have access through the bridges to the disk shelves in each stack.

- You should hot-add an equal number of disk shelves at each site.
- 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.

> Starting with ONTAP 9.8, the **`storage bridge`** command is replaced with **`system bridge`**. The following steps show the **`storage bridge`** command, but if you are running ONTAP 9.8 or later, the **`system bridge`** command is preferred.

> If you insert a SAS cable into the wrong port, when you remove the cable from a SAS port, you must wait at least 120 seconds before plugging the cable into a different SAS port. If you fail to do so, the system will not recognize that the cable has been moved to another port.

Steps

1. Properly ground yourself.
2. From the console of either controller module, check whether your system has disk autoassignment enabled:

   `storage disk option show`

   The Auto Assign column indicates whether disk autoassignment is enabled.

   ```
   Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
   ----------  -------------  ----------  -----------  ------------------
   node_A_1             on           on           on           default
   node_A_2             on           on           on           default
   2 entries were displayed.
   ```

3. Disable the switch ports for the new stack.
4. 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.

5. 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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

   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.

6. Configure the bridge.

   If you retrieved the configuration information from the old bridge, use the information to configure the new bridge.

   Be sure to make note of the user name and password that you designate.

The *ATTO FibreBridge Installation and Operation Manual* for your bridge model has the most current information on available commands and how to use them.

> 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.

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

   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 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`

   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. Starting with ONTAP 9.8, only in-band management is supported and SNMP management is deprecated.

7. 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.

> ⓘ The FCDataRate speed you select is limited to the maximum speed supported by both the bridge and the switch to which the bridge port connects. Cabling distances must not exceed the limitations of the SFPs and other hardware.

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.

> ⓘ The FCConnMode setting is not required when configuring a FibreBridge 7600N bridge.

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`***

d. If you are configuring a FibreBridge 7600N or 7500N bridge, disable the unused SAS ports:
`SASPortDisable` ***`sas-port`***

> ⓘ SAS ports A through D are enabled by default. You must disable the SAS ports that are not being used. If only SAS port A is used, then SAS ports B, C, and D must be disabled.

8. Secure access to the bridge and save the bridge's configuration.

a. From the controller prompt check the status of the bridges:

`storage bridge show`

The output shows which bridge is not secured.

b. Check the status of the unsecured bridge's ports:
`info`

The output shows the status of Ethernet ports MP1 and MP2.

c. If Ethernet port MP1 is enabled, run the following command:
`set EthernetPort mp1 disabled`

> ⓘ If Ethernet port MP2 is also enabled, repeat the previous substep for port MP2.

d. Save the bridge’s configuration.

   You must run the following commands:

   SaveConfiguration

   FirmwareRestart

   You are prompted to restart the bridge.

9. Update the FibreBridge firmware on each bridge.

   If the new bridge is the same type as the partner bridge upgrade to the same firmware as the partner bridge. If the new bridge is a different type to the partner bridge, upgrade to the latest firmware supported by the bridge and version of ONTAP. See the section "Updating firmware on a FibreBridge bridge" in the *MetroCluster Maintenance Guide*.

10. Cable the disk shelves to the bridges:

    a. Daisy-chain the disk shelves in each stack.

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

    b. For each stack of disk shelves, cable IOM A of the first shelf to SAS port A on FibreBridge A, and then cable IOM B of the last shelf to SAS port A on FibreBridge B.

       Fabric-attached MetroCluster installation and configuration

       Stretch MetroCluster installation and configuration

       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.

       > The bridge SAS port B is disabled.

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

If you are using the…	Then…
ATTO ExpressNAV GUI	a. In a supported web browser, enter the IP address of a bridge in the browser box. You are brought to the ATTO FibreBridge home page, which has a link. 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 appears with a menu to the left. c. Click **Advanced** in the menu. d. View the connected devices: **`sastargets`** e. Click **Submit**.
Serial port connection	View the connected devices: **`sastargets`**

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

If the text response truncated appears at the beginning of the output, you can use Telnet to connect to the bridge, and then view all of the output by using the sastargets command.

The following output shows that 10 disks are connected:

```
Tgt VendorID ProductID        Type        SerialNumber
  0 NETAPP   X410_S15K6288A15 DISK        3QP1CLE300009940UHJV
  1 NETAPP   X410_S15K6288A15 DISK        3QP1ELF600009940V1BV
  2 NETAPP   X410_S15K6288A15 DISK        3QP1G3EW00009940U2M0
  3 NETAPP   X410_S15K6288A15 DISK        3QP1EWMP00009940U1X5
  4 NETAPP   X410_S15K6288A15 DISK        3QP1FZLE00009940G8YU
  5 NETAPP   X410_S15K6288A15 DISK        3QP1FZLF00009940TZKZ
  6 NETAPP   X410_S15K6288A15 DISK        3QP1CEB400009939MGXL
  7 NETAPP   X410_S15K6288A15 DISK        3QP1G7A900009939FNTT
  8 NETAPP   X410_S15K6288A15 DISK        3QP1FY0T00009940G8PA
  9 NETAPP   X410_S15K6288A15 DISK        3QP1FXW600009940VERQ
```

12. Verify that the command output shows that the bridge is connected to all of the appropriate disks and disk shelves in the stack.

If the output is…	Then…
Correct	Repeat Step 11 for each remaining bridge.
Not correct	a. Check for loose SAS cables or correct the SAS cabling by repeating Step 10. b. Repeat Step 11.

13. If you are configuring a fabric-attached MetroCluster configuration, cable each bridge to the local FC switches, using the cabling shown in the table for your configuration, switch model, and FC-to-SAS bridge model:

> Brocade and Cisco switches use different port numbering, as shown in the following tables.

   - On Brocade switches, the first port is numbered “0”.
   - On Cisco switches, the first port is numbered “1”.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)												
DR GROUP 1												
			Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Component		Port	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2
Stack 1	bridge _x_1a	FC1	8		8		8		8		10	
		FC2	-	8	-	8	-	8	-	8	-	10
	bridge _x_1B	FC1	9	-	9	-	9	-	9	-	11	-
		FC2	-	9	-	9	-	9	-	9	-	11
Stack 2	bridge _x_2a	FC1	10	-	10	-	10	-	10	-	14	-
		FC2	-	10	-	10	-	10	-	10	-	14
	bridge _x_2B	FC1	11	-	11	-	11	-	11	-	17	-
		FC2	-	11	-	11	-	11	-	11	-	17

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)												
Stack 3	bridge _x_3a	FC1	12	-	12	-	12	-	12	-	18	-
		FC2	-	12	-	12	-	12	-	12	-	18
	bridge _x_3B	FC1	13	-	13	-	13	-	13	-	19	-
		FC2	-	13	-	13	-	13	-	13	-	19
Stack y	bridge _x_ya	FC1	14	-	14	-	14	-	14	-	20	-
		FC2	-	14	-	14	-	14	-	14	-	20
	bridge _x_yb	FC1	15	-	15	-	15	-	15	-	21	-
		FC2		15		15		15	-	15	-	21

Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620, G630, G620-1, and G630-1 switches.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)										
DR GROUP 2										
			Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G720	
Component		Port	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	switch 2
Stack 1	bridge_ x_51a	FC1	26	-	32	-	56	-	32	-
		FC2	-	26	-	32	-	56	-	32
	bridge_ x_51b	FC1	27	-	33	-	57	-	33	-
		FC2	-	27	-	33	-	57	-	33

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

Stack 2	bridge_x_52a	FC1	30	-	34	-	58	-	34	-
		FC2	-	30	-	34	-	58	-	34
	bridge_x_52b	FC1	31	-	35	-	59	-	35	-
		FC2	-	31	-	35	-	59	-	35
Stack 3	bridge_x_53a	FC1	32	-	36	-	60	-	36	-
		FC2	-	32	-	36	-	60	-	36
	bridge_x_53b	FC1	33	-	37	-	61	-	37	-
		FC2	-	33	-	37	-	61	-	37
Stack y	bridge_x_5ya	FC1	34	-	38	-	62	-	38	-
		FC2	-	34	-	38	-	62	-	38
	bridge_x_5yb	FC1	35	-	39	-	63	-	39	-
		FC2	-	35	-	39	-	63	-	39

Additional bridges can be cabled to ports 36 - 39 in G620, G630, G620-1, and G-630-1 switches.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only

DR GROUP 1											
		Brocade 6505		Brocade 6510, Brocade DCX 8510-8		Brocade 6520		Brocade G620, brocade G620-1, Brocade G630, Brocade G630-1		Brocade G720	
Component	Port	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2	Switch 1	Switch 2
Stack 1	bridge_x_1a	8		8		8		8		10	
	bridge_x_1b	-	8	-	8	-	8	-	8	-	10

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only											
Stack 2	bridge _x_2a	9	-	9	-	9	-	9	-	11	-
	bridge _x_2b	-	9	-	9	-	9	-	9	-	11
Stack 3	bridge _x_3a	10	-	10	-	10	-	10	-	14	-
	bridge _x_4b	-	10	-	10	-	10	-	10	-	14
Stack y	bridge _x_ya	11	-	11	-	11	-	11	-	15	-
	bridge _x_yb	-	11	-	11	-	11	-	11	-	15

Additional bridges can be cabled to ports 12 - 17, 20 and 21 in G620, G630, G620-1, and G630-1 switches. Additional bridges can be cabled to ports 16 - 17, 20 and 21 G720 switches.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only									
DR GROUP 2									
		Brocade G720		Brocade G620, Brocade G620-1, Brocade G630, Brocade G630-1		Brocade 6510, Brocade DCX 8510-8		Brocade 6520	
Stack 1	bridge_x _51a	32	-	26	-	32	-	56	-
	bridge_x _51b	-	32	-	26	-	32	-	56
Stack 2	bridge_x _52a	33	-	27	-	33	-	57	-
	bridge_x _52b	-	33	-	27	-	33	-	57

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only									
Stack 3	bridge_x_53a	34	-	30	-	34	-	58	-
	bridge_x_54b	-	34	-	30	-	34	-	58
Stack y	bridge_x_ya	35	-	31	-	35	-	59	-
	bridge_x_yb	-	35	-	31	-	35	-	59

Additional bridges can be cabled to ports 32 - 39 in G620, G630, G620-1, and G630-1 switches. Additional bridges can be cabled to ports 36 - 39 in G720 switches.

14. If you are configuring a bridge-attached MetroCluster system, cable each bridge to the controller modules:
    a. Cable FC port 1 of the bridge to a 16 Gb or 8 Gb FC port on the controller module in cluster_A.
    b. Cable FC port 2 of the bridge to the same speed FC port of the controller module in cluster_A.
    c. Repeat these substeps on other subsequent bridges until all of the bridges have been cabled.
15. Update the disk drive firmware to the most current version from the system console:

    `disk_fw_update`

    You must run this command on both controller modules.

    NetApp Downloads: Disk Drive Firmware

16. Update the disk shelf firmware to the most current version by using the instructions for the downloaded firmware.

    You can run the commands in the procedure from the system console of either controller module.

    NetApp Downloads: Disk Shelf Firmware

17. If your system does not have disk autoassignment enabled, assign disk drive ownership.

    Disk and aggregate management

    If you are splitting the ownership of a single stack of disk shelves among multiple controller modules, you must disable disk autoassignment on both nodes in the cluster (`storage disk option modify -autoassign off *`) before assigning disk ownership; otherwise, when you assign any single disk drive, the remaining disk drives might be automatically assigned to the same controller module and pool.

> You must not add disk drives to aggregates or volumes until after the disk drive firmware and disk shelf firmware have been updated and the verification steps in this task have been completed.

18. Enable the switch ports for the new stack.
19. Verify the operation of the MetroCluster configuration in ONTAP:
    a. Check whether the system is multipathed:
       `node run -node *node-name* sysconfig -a`
    b. Check for any health alerts on both clusters:
       `system health alert show`
    c. Confirm the MetroCluster configuration and that the operational mode is normal:
       `metrocluster show`
    d. Perform a MetroCluster check:
       `metrocluster check run`
    e. Display the results of the MetroCluster check:
       `metrocluster check show`
    f. Check for any health alerts on the switches (if present):
       `storage switch show`
    g. Run Config Advisor.

       NetApp Downloads: Config Advisor
    h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
20. If applicable, repeat this procedure for the partner site.

Related information

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

Hot-adding a SAS disk shelf to a stack of SAS disk shelves

You can hot-add one or more SAS disk shelves to a stack of SAS disk shelves.

Preparing to hot-add SAS disk shelves

Preparing to hot-add a SAS disk shelf involves downloading documents as well as the disk drive and disk shelf firmware.

- Your system must be a supported configuration and must be running a supported version of ONTAP.
- All disk drives and disk shelves in the system must be running the latest firmware version.

  You might want to update the disk and shelf firmware throughout the MetroCluster configuration prior to adding shelves.

  Upgrade, revert, or downgrade

A mix of IOM12 modules and IOM6 modules is supported within the same stack if your system is running a supported version of ONTAP. To establish whether your version of ONTAP supports shelf mixing, refer to the Interoperability Matrix Tool (IMT).https://mysupport.netapp.com/NOW/products/interoperability[NetApp Interoperability] If your version of ONTAP is not supported and you cannot upgrade or downgrade the IOM modules on the existing stack or the new shelf that is to be added to a supported combination of IOM modules, you need to do one of the following:

- Start a new stack on a new SAS port (if supported by the bridge-pair).
- Start a new stack on an additional bridge-pair.

Steps

1. Download or view the following documents from the NetApp Support Site:
   - NetApp Interoperability Matrix Tool
   - The *Installation Guide* for your disk shelf model.
2. Verify that the disk shelf you are hot-adding is supported.

   NetApp Interoperability Matrix Tool
3. Download the latest disk and disk shelf firmware:

   In this step, you are only completing the download portion of the instructions provided in the links. You need to follow the steps found in the Hot-adding a disk shelf section for installing the disk shelf.

   a. Download the disk firmware and make a copy of the disk firmware instructions for reference later.

      NetApp Downloads: Disk Drive Firmware

   b. Download the disk shelf firmware and make a copy of the disk shelf firmware instructions for reference later.

      NetApp Downloads: Disk Shelf Firmware

Hot-adding a disk shelf

You can hot-add a disk shelf when you want to increase storage without any reduction in performance.

- The system must meet all of the requirements in Preparing to hot-add SAS disk shelves.
- Your environment must meet one of the following scenarios to hot-add a shelf:
  - You have two FibreBridge 7500N bridges connected to a stack of SAS disk shelves.
  - You have one FibreBridge 7500N bridge and one FibreBridge 6500N bridge connected to a stack of SAS disk shelves.
  - You have two FibreBridge 6500N bridges connected to a stack of SAS disk shelves.
- This procedure is for hot-adding a disk shelf to the last disk shelf in a stack.

  This procedure is written with the assumption that the last disk shelf in a stack is connected from IOM A to bridge A and from IOM B to bridge B.

- This is a nondisruptive procedure.
- You should hot-add an equal number of disk shelves at each site.
- If you are hot-adding more than one disk shelf, you must hot-add one disk shelf at a time.

> Each pair of FibreBridge 7500N or 7600N bridges can support up to four stacks.

> Hot-adding a disk shelf requires you to update the disk drive firmware on the hot-added disk shelf by running the `storage disk firmware update` command in advanced mode. Running this command can be disruptive if the firmware on existing disk drives in your system is an older version.

> If you insert a SAS cable into the wrong port, when you remove the cable from a SAS port, you must wait at least 120 seconds before plugging the cable into a different SAS port. If you fail to do so, the system will not recognize that the cable has been moved to another port.

Steps

1. Properly ground yourself.
2. Verify disk shelf connectivity from the system console of either controller:

   `sysconfig -v`

   The output is similar to the following:

   - Each bridge on a separate line and under each FC port to which it is visible; for example, hot-adding a disk shelf to a set of FibreBridge 7500N bridges results in the following output:

     ```
     FC-to-SAS Bridge:
     cisco_A_1-1:9.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100189
     cisco_A_1-2:1.126L0: ATTO  FibreBridge7500N 2.10  FB7500N100162
     ```

   - Each disk shelf on a separate line under each FC port to which it is visible:

     ```
     Shelf   0: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
     Shelf   1: IOM6  Firmware rev. IOM6 A: 0173 IOM6 B: 0173
     ```

   - Each disk drive on a separate line under each FC port to which it is visible:

     ```
     cisco_A_1-1:9.126L1   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
     (879097968 520B/sect)
     cisco_A_1-1:9.126L2   : NETAPP   X421_HCOBD450A10 NA01 418.0GB
     (879097968 520B/sect)
     ```

3. Check whether your system has disk autoassignment enabled from the console of either controller:

storage disk option show

The autoassignment policy is shown in the Auto Assign column.

```
Node         BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on          on           on           default
node_A_2             on          on           on           default
2 entries were displayed.
```

4. If your system does not have disk autoassignment enabled, or if disk drives in the same stack are owned by both controllers, assign disk drives to the appropriate pools.

   Disk and aggregate management

   > If you are splitting a single stack of disk shelves between two controllers, disk autoassignment must be disabled before you assign disk ownership; otherwise, when you assign any single disk drive, the remaining disk drives might be automatically assigned to the same controller and pool.
   >
   > The `storage disk option modify -node` *`node-name`* `-autoassign off` command disables disk autoassignment.

   > Disk drives must not be added to aggregates or volumes until the disk drive and disk shelf firmware have been updated.

5. Update the disk shelf firmware to the most current version by using the instructions for the downloaded firmware.

   You can run the commands in the procedure from the system console of either controller.

   NetApp Downloads: Disk Shelf Firmware

6. Install and cable the disk shelf:

   Note the following considerations:

   - For FibreBridge 6500N bridges:

     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).

   - For FibreBridge 7500N bridges:

     Do not force a connector into a port. The mini-SAS cables are keyed; when oriented correctly into a SAS port, the SAS cable 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 up (on the topside of the connector).

a. Install the disk shelf, power it on, and set the shelf ID.

   The *Installation Guide* for your disk shelf model provides detailed information about installing disk shelves.

   > You must power-cycle the disk shelf and keep the shelf IDs unique for each SAS disk shelf within the entire storage system.

b. Disconnect the SAS cable from the IOM B port of the last shelf in the stack, and then reconnect it to the same port in the new shelf.

   The other end of this cable remains connected to bridge B.

c. Daisy-chain the new disk shelf by cabling the new shelf IOM ports (of IOM A and IOM B) to the last shelf IOM ports (of IOM A and IOM B).

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

7. Update the disk drive firmware to the most current version from the system console.

   NetApp Downloads: Disk Drive Firmware

   a. Change to the advanced privilege level:
      `set -privilege advanced`

      You need to respond with **`y`** when prompted to continue into advanced mode and see the advanced mode prompt (*>).

   b. Update the disk drive firmware to the most current version from the system console:
      `storage disk firmware update`

   c. Return to the admin privilege level:
      `set -privilege admin`

   d. Repeat the previous substeps on the other controller.

8. Verify the operation of the MetroCluster configuration in ONTAP:

   a. Check whether the system is multipathed:

      `node run -node` *`node-name`* `sysconfig -a`

   b. Check for any health alerts on both clusters:
      `system health alert show`

   c. Confirm the MetroCluster configuration and that the operational mode is normal:
      `metrocluster show`

   d. Perform a MetroCluster check:
      `metrocluster check run`

   e. Display the results of the MetroCluster check:

      `metrocluster check show`

   f. Check for any health alerts on the switches (if present):

```
storage switch show
```

g. Run Config Advisor.

   NetApp Downloads: Config Advisor

h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

9. If you are hot-adding more than one disk shelf, repeat the previous steps for each disk shelf that you are hot-adding..

Hot-adding an IOM12 disk shelf to a stack of IOM6 disk shelves in a bridge-attached MetroCluster configuration

Depending on your version of ONTAP, you can hot-add an IOM12 disk shelf to a stack of IOM6 disk shelves in a bridge-attached MetroCluster configuration.

To perform this procedure, see Hot-adding shelves with IOM12 modules to a stack of shelves with IOM6 modules.

Hot-removing storage from a MetroCluster FC configuration

You can hot-remove drive shelves—physically remove shelves that have had the aggregates removed from the drives—from a MetroCluster FC configuration that is up and serving data. You can hot-remove one or more shelves from anywhere within a stack of shelves or remove a stack of shelves.

- Your system must be a multipath HA, multipath, quad-path HA, or quad-path configuration.
- In a four-node MetroCluster FC configuration, the local HA pair cannot be in a takeover state.
- You must have already removed all aggregates from the drives in the shelves that you are removing.

  > If you attempt this procedure on non-MetroCluster FC configurations with aggregates on the shelf you are removing, you could cause the system to fail with a multidrive panic.

  Removing aggregates involves splitting the mirrored aggregates on the shelves you are removing, and then re-creating the mirrored aggregates with another set of drives.

  Disk and aggregate management

- You must have removed drive ownership after removing the aggregates from the drives in the shelves that you are removing.

  Disk and aggregate management

- If you are removing one or more shelves from within a stack, you must have factored the distance to bypass the shelves that you are removing.

  If the current cables are not long enough, you need to have longer cables available.

This task applies to the following MetroCluster FC configurations:

- Direct-attached MetroCluster FC configurations, in which the storage shelves are directly connected to the storage controllers with SAS cables
- Fabric-attached or bridge-attached MetroCluster FC configurations, in which the storage shelves are connected using FC-to-SAS bridges

Steps

1. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:
      `node run -node` ***`node-name`*** **`sysconfig -a`**
   b. Check for any health alerts on both clusters:

      `system health alert show`

   c. Confirm the MetroCluster configuration and that the operational mode is normal:
      `metrocluster show`
   d. Perform a MetroCluster check:

      `metrocluster check run`

   e. Display the results of the MetroCluster check:

      `metrocluster check show`

   f. Check for any health alerts on the switches (if present):

      `storage switch show`

   g. Run Config Advisor.

      NetApp Downloads: Config Advisor

   h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
2. Set the privilege level to advanced:

   `set -privilege advanced`

3. Verify that no mailbox drive is on the shelves: **`storage failover mailbox-disk show`**
4. Remove the shelf according to the steps for the relevant scenario.

Scenario	Steps
To remove an aggregate when the shelf contains either unmirrored, mirrored, or both types of aggregate…	a. Use the **`storage aggregate delete -aggregate`** ***`aggregate name`*** command to remove the aggregate. b. Use the standard procedure to remove ownership of all drives in that shelf, and then physically remove the shelf. Follow the instructions in the *SAS Disk Shelves Service Guide* for your shelf model to hot-remove shelves.

<table>
<tr><th>Scenario</th><th>Steps</th></tr>
<tr><td>To remove a plex from a mirrored aggregate, you need to unmirror the aggregate.</td><td>

a. Identify the plex that you want to remove by using the **run -node local sysconfig -r** command.

In the following example, you can identify the plex from the line `Plex /dpg_mcc_8020_13_a1_aggr1/plex0`. In this case, the plex to specify is plex0.

```
dpgmcc_8020_13_a1a2::storage
aggregate> run -node local
sysconfig -r
*** This system has taken over
dpg-mcc-8020-13-a1
Aggregate
dpg_mcc_8020_13_a1_aggr1
(online, raid_dp, mirrored)
(block checksums)
  Plex
/dpg_mcc_8020_13_a1_aggr1/plex
0 (online, normal, active,
pool0)
    RAID group
/dpg_mcc_8020_13_a1_aggr1/plex
0/rg0 (normal, block
checksums)
      RAID Disk Device
HA  SHELF BAY CHAN Pool Type
RPM  Used (MB/blks)    Phys
(MB/blks)
      --------- ------
------------- ---- ---- ----
----- --------------
--------------
      dparity   mcc-cisco-8Gb-
fab-2:1-1.126L16  0c    32  15
FC:B   0   SAS 15000
272000/557056000
274845/562884296
      parity    mcc-cisco-8Gb-
fab-2:1-1.126L18  0c    32  17
FC:B   0   SAS 15000
272000/557056000
274845/562884296
      data      mcc-cisco-8Gb-
fab-2:1-1.126L19  0c    32  18
FC:B   0   SAS 15000
272000/557056000
```

</td></tr>
</table>

Replacing a shelf nondisruptively in a stretch MetroCluster configuration

You can replace disk shelves without disruption in a stretch MetroCluster configuration with a fully populated disk shelf or a disk shelf chassis and transfer components from the shelf you are removing.

The disk shelf model you are installing must meet the storage system requirements specified in the Hardware Universe, which includes supported shelf models, supported disk drive types, the maximum number of disk shelves in a stack, and supported ONTAP versions.

Steps

1. Properly ground yourself.
2. Identify all aggregates and volumes that have disks from the loop that contains the shelf you are replacing and make note of the affected plex name.

   Either node might contain disks from the loop of the affected shelf and host aggregates or host volumes.

3. Choose one of the following two options based on the replacement scenario you are planning.
   - If you are replacing a complete disk shelf, including the shelf chassis, disks, and I/O modules (IOM), take the corresponding action as described in the table below:

Scenario	Action
The affected plex contains fewer disks from the affected shelf.	Replace the disks one-by-one on the affected shelf with spares from another shelf. You can take the plex offline after completing the disk replacement.
The affected plex contains more disks than are in the affected shelf.	Move the plex offline and then delete the plex.
The affected plex has any disk from the affected shelf.	Move the plex offline but do not delete it.

   - If you are replacing only the disk shelf chassis and no other components, perform the following steps:
     a. Offline the affected plexes from the controller where they are hosted:
        `aggregate offline`
     b. Verify that the plexes are offline:

        `aggregate status -r`

4. Identify the controller SAS ports to which the affected shelf loop is connected and disable the SAS ports on both site controllers:

   `storage port disable -node *node_name* -port *SAS_port*`

   The affected shelf loop is connected to both sites.

```
274845/562884296
      data      mcc-cisco-8Gb-
fab-2:1-1.126L21  0c    32  20
FC:B   0   SAS 15000
272000/557056000
274845/562884296
      data      mcc-cisco-8Gb-
fab-2:1-1.126L22  0c    32  21
FC:B   0   SAS 15000
272000/557056000
274845/562884296

  Plex
/dpg_mcc_8020_13_a1_aggr1/plex
1 (online, normal, active,
pool1)
   RAID group
/dpg_mcc_8020_13_a1_aggr1/plex
1/rg0 (normal, block

272000/557056000
280104/573653840
      parity    mcc-cisco-8Gb-
fab-3:1-1.126L14  0d    33  13
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      data      mcc-cisco-8Gb-
fab-3:1-1.126L41  0d    33  41
FC:A   1   SAS 15000
272000/557056000
280104/573653840
      data      mcc-cisco-8Gb-
fab-3:1-1.126L15  0d    33  14
FC:A   1   SAS 15000
272000/557056000
```

5. Wait for ONTAP to recognize that the disk is missing. You can use the following commands to verify that the disk is missing: **`sysconfig -a`** or **`sysconfig -r`**.
6. Turn off the power switch on the disk shelf.
7. Unplug all power cords from the disk shelf.
8. Make a record of the ports from which you unplug the cables so that you can cable the new disk shelf in the same way.
9. Unplug and remove the cables connecting the disk shelf to the other disk shelves or the storage system.
10. Remove the disk shelf from the rack.

    To make the disk shelf lighter and easier to maneuver, remove the power supplies and IOM. If you will be installing a disk shelf chassis, also remove the disk drives or carriers. Otherwise, avoid removing disk drives or carriers if possible because excessive handling can cause internal drive damage.

11. Install and secure the replacement disk shelf onto the support brackets and rack.
12. If you installed a disk shelf chassis, reinstall power supplies and IOM.
13. Reconfigure the stack of disk shelves by connecting all cables to the replacement disk shelf ports exactly as they were configured on the disk shelf that you removed.
14. Turn on the power to the replacement disk shelf and wait for the disk drives to spin up.
15. Change the disk shelf ID to a unique ID from 0 through 98.
16. Enable any SAS ports that you previously disabled and then wait for ONTAP to recognize that the disks are inserted.

    You can use the following commands to verify that the disks are inserted: **`sysconfig -a`** or **`sysconfig -r`** .

17. If you are replacing the complete disk shelf (disk shelf chassis, disks, IOM), perform the following steps:

    > If you are replacing only the disk shelf chassis and no other components, go to Step 19.

    a. Use the **`storage disk option modify -autoassign`** command to determine whether disk auto assignment is enabled (on).

       Disk assignment will occur automatically.

    b. If disk auto assignment is not enabled, assign disk ownership manually.

18. Move the plexes back online: **`aggregate online`** ***`plex name`***
19. Recreate any plexes that were deleted by mirroring the aggregate.
20. Monitor the plexes as they begin resynchronizing:

    `aggregate status -r <aggregate name>`

21. Verify that the storage system is functioning as expected:

    `system health alert show`

```
280104/573653840
        data      mcc-cisco-8Gb-
fab-3:1-1.126L45  0d    34  18
FC:A   1   SAS  15000
272000/557056000
280104/573653840
```

b. Use the **`storage aggregate plex delete -aggregate`** ***`aggr_name`*** **`-plex`** ***`plex_name`*** command to remove the plex.

plex defines the plex name, such as `plex3` or `plex6`.

c. Use the standard procedure to remove ownership of all drives in that shelf, and then physically remove the shelf.

Follow the instructions in the *SAS Disk Shelves Service Guide* for your shelf model to hot-remove shelves.

Replacing a shelf nondisruptively in a fabric-attached MetroCluster configuration

You might need to know how to replace a shelf nondisruptively in a fabric-attached MetroCluster configuration.

> This procedure is only for use in a fabric-attached MetroCluster configuration.

Disabling access to the shelf

You must disable access to the shelf before you replace the shelf modules.

Check the overall health of the configuration. If the system does not appear healthy, address the issue first before proceeding.

Steps

1. Offline the affected plexes on the controller where they are hosted:

   `aggr offline` ***`plex_name`***

   The example shows the commands for offlining plexes for a controller running cMode.

   ```
   Cluster_A_1::> storage aggregate plex offline -aggr aggr1 -plex plex2
   Cluster_A_1::> storage aggregate plex offline -aggr aggr2 -plex plex6
   Cluster_A_1::> storage aggregate plex offline -aggr aggr3 -plex plex1
   ```

2. Verify that the plexes are offline:

   `aggr status` ***`-raggr_name`***

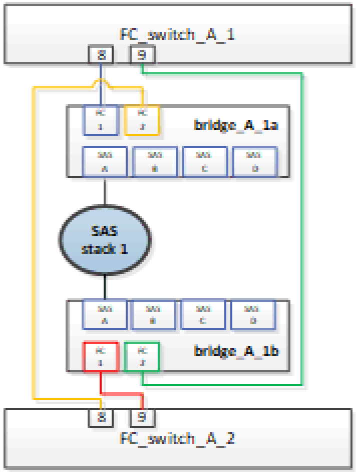
   The example shows the commands for verifying that the aggregates are offline for a controller running cMode.

   ```
   Cluster_A_1::> storage aggregate show -aggr aggr1
   Cluster_A_1::> storage aggregate show -aggr aggr2
   Cluster_A_1::> storage aggregate show -aggr aggr3
   ```

3. Disable the SAS ports or switch ports depending on whether the bridges connecting the target shelf are connecting a single SAS stack or two or more SAS stacks:

   - If the bridges are connecting a single SAS stack, disable the switch ports that the bridges are connected to using the appropriate command for your switch.

     The following example shows a pair of bridges that connect a single SAS stack, which contains the target shelf:



Switch ports 8 and 9 on each switch connect the bridges to the network.

The following example shows ports 8 and 9 being disabled on a Brocade switch.

```
FC_switch_A_1:admin> portDisable 8
FC_switch_A_1:admin> portDisable 9

FC_switch_A_2:admin> portDisable 8
FC_switch_A_2:admin> portDisable 9
```

The following example shows port 8 and 9 being disabled on a Cisco switch.

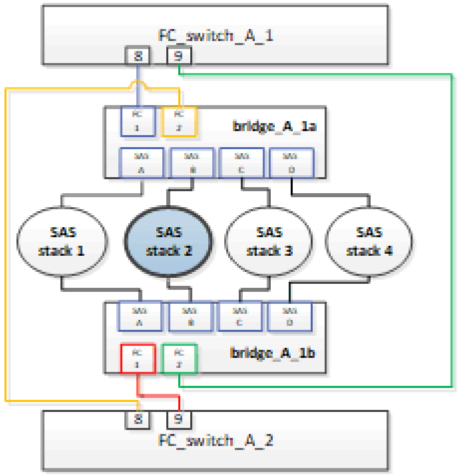
```
FC_switch_A_1# conf t
FC_switch_A_1(config)# int fc1/8
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# int fc1/9
FC_switch_A_1(config)# shut
FC_switch_A_1(config)# end

FC_switch_A_2# conf t
FC_switch_A_2(config)# int fc1/8
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# int fc1/9
FC_switch_A_2(config)# shut
FC_switch_A_2(config)# end
```

◦ If the bridges are connecting two or more SAS stacks, disable the SAS ports connecting the bridges to the target shelf:
SASportDisable *port number*

This is not applicable to FibreBridge 6500 bridges.

The following example shows a pair of bridges that connect four SAS stacks. SAS stack 2 contains the target shelf:



SAS port B connects the bridges to the target shelf. By disabling only SAS port B on both shelves, the other SAS stacks can continue to serve data during the replacement procedure.

In this case, disable the SAS port connecting the bridge to the target shelf:

`SASportDisable` ***`port number`***

The following example shows SAS port B being disabled from the bridge and also verifies that it is disabled. You must repeat the command on both bridges.

```
Ready. *
SASPortDisable B

SAS Port B has been disabled.
```

4. If you previously disabled the switch ports, verify that they are disabled:

   `switchShow`

   The example shows that the switch ports are disabled on a Brocade switch.

```
FC_switch_A_1:admin> switchShow
FC_switch_A_2:admin> switchShow
```

   The example shows that the switch ports are disabled on a Cisco switch.

```
FC_switch_A_1# show interface fc1/6
FC_switch_A_2# show interface fc1/6
```

5. Wait for ONTAP to realize that the disk is missing.
6. Power off the shelf that you want to replace.

Replacing the shelf

You must physically remove all of the cables and the shelf before inserting and cabling the new shelf and shelf modules.

Steps

1. Remove all disks and disconnect all cables from the shelf that is being replaced.
2. Remove the shelf modules.
3. Insert the new shelf.
4. Insert the new disks into the new shelf.
5. Insert the shelf modules.
6. Cable the shelf (SAS or Power).
7. Power on the shelf.

Reenabling access and verifying the operation

After the shelf has been replaced, you need to reenable access and verify that the new shelf is operating correctly.

Steps

1. Verify that the shelf powers properly and the links on the IOM modules are present.
2. Enable the switch ports or SAS port according to the following scenarios:

<table>
<tr><th>Option</th><th>Step</th></tr>
<tr><td>If you previously disabled switch ports</td><td>

a. Enable the switch ports: <code>portEnable port number</code> The example shows the switch port being enabled on a Brocade switch.

<pre><code>Switch_A_1:admin> portEnable 6
Switch_A_2:admin> portEnable 6</code></pre>

The example shows the switch port being enabled on a Cisco switch.

<pre><code>Switch_A_1# conf t
Switch_A_1(config)# int fc1/6
Switch_A_1(config)# no shut
Switch_A_1(config)# end

Switch_A_2# conf t
Switch_A_2(config)# int fc1/6
Switch_A_2(config)# no shut
Switch_A_2(config)# end</code></pre>

</td></tr>
<tr><td>If you previously disabled a SAS port</td><td>

a. Enable the SAS port connecting the stack to the shelf location:
<code>SASportEnable port number</code>

The example shows SAS port A being enabled from the bridge and also verifies that it is enabled.

<pre><code>Ready. *
SASPortEnable A

SAS Port A has been enabled.</code></pre>

ⓘ This is not applicable to ATTO 6500 FibreBridges.

</td></tr>
</table>

3. If you previously disabled the switch ports, verify that they are enabled and online and that and all devices are logged in correctly:

   `switchShow`

   The example shows the **`switchShow`** command for verifying that a Brocade switch is online.

```
Switch_A_1:admin> SwitchShow
Switch_A_2:admin> SwitchShow
```

The example shows the **switchShow** command for verifying that a Cisco switch is online.

```
Switch_A_1# show interface fc1/6
Switch_A_2# show interface fc1/6
```

> After several minutes, ONTAP detects that new disks have been inserted and displays a message for each new disk.

4. Verify that the disks have been detected by ONTAP:

   sysconfig -a

5. Online the plexes that were offline earlier:

   aggr online*plex_name*

   The example shows the commands for placing plexes on a controller running cMode back online.

```
Cluster_A_1::> storage aggregate plex online -aggr aggr1 -plex plex2
Cluster_A_1::> storage aggregate plex online -aggr aggr2 -plex plex6
Cluster_A_1::> storage aggregate plex online -aggr aggr3 -plex plex1
```

   The plexes begin to resynchronize.

> You can monitor the progress of resynchronization using the **aggr status -r*aggr_name*** command.

When to migrate root volumes to a new destination

You might need to move root volumes to another root aggregate within a two-node or four-node MetroCluster configuration.

Migrating root volumes within a two-node MetroCluster configuration

To migrate root volumes to a new root aggregate within a two-node MetroCluster configuration, you should refer to How to move mroot to a new root aggregate in a 2-node Clustered MetroCluster with Switchover. This procedure shows you how to non-disruptively migrate the root volumes during a MetroCluster switchover operation. This procedure is slightly different than the procedure used on a four-node configuration.

Migrating root volumes within a four-node MetroCluster configuration

To migrate root volumes to a new root aggregate within a four-node MetroCluster configuration, you can use the system node migrate-root command while meeting the following requirements.

- You can use system node migrate-root to move root aggregates within a four-node MetroCluster configuration.
- All root aggregates must be mirrored.
- You can add new shelves on both sites with smaller drives to host the root aggregate.
- You must check the drive limits that the platform supports before attaching new drives.

  NetApp Hardware Universe

- If you move the root aggregate to smaller drives, you need to accommodate the minimum root volume size of the platform to ensure all core files are saved.

> The four-node procedure can also be applied to an eight-node configuration.

Moving a metadata volume in MetroCluster configurations

You can move a metadata volume from one aggregate to another aggregate in a MetroCluster configuration. You might want to move a metadata volume when the source aggregate is decommissioned or unmirrored, or for other reasons that make the aggregate ineligible.

- You must have cluster administrator privileges to perform this task.
- The target aggregate must be mirrored and should not be in the degraded state.
- The available space in the target aggregate must be larger than the metadata volume that you are moving.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Identify the metadata volume that should be moved:

   `volume show MDV_CRS*`

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW            -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW            -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Identify an eligible target aggregate:

   `metrocluster check config-replication show-aggregate-eligibility`

   The following command identifies the aggregates in cluster_A that are eligible to host metadata volumes:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

> In the previous example, Node_A_1_aggr2 and Node_A_2_aggr2 are eligible.

4. Start the volume move operation:

volume move start -vserver *svm_name* -volume *metadata_volume_name* -destination -aggregate *destination_aggregate_name*

The following command moves metadata volume `MDV_CRS_14c00d4ac9f311e7922800a0984395f1` from `aggregate Node_A_1_aggr1` to `aggregate Node_A_1_aggr2`:

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Verify the state of the volume move operation:

   volume move show -volume vol_constituent_name

6. Return to the admin privilege level:

   set -privilege admin

Renaming a cluster in MetroCluster configurations

Renaming a cluster in a MetroCluster configuration involves making the changes, and then verifying on both the local and remote clusters that the change took effect correctly.

Steps

1. View the cluster names using the

   metrocluster node show

   command:

```
cluster_1::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_1
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
      cluster_2
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
4 entries were displayed.
```

2. Rename the cluster:

   cluster identity modify -name *new_name*

   In the following example, the `cluster_1` cluster is renamed `cluster_A`:

```
cluster_1::*> cluster identity modify -name cluster_A
```

3. Verify on the local cluster that the renamed cluster is running normally:

   metrocluster node show

   In the following example, the newly renamed `cluster_A` is running normally:

```
cluster_A::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
      cluster_2
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
4 entries were displayed.
```

4. Rename the remote cluster:

   cluster peer modify-local-name -name *cluster_2* -new-name *cluster_B*

   In the following example, `cluster_2` is renamed `cluster_B`:

```
cluster_2::> cluster peer modify-local-name -name cluster_2 -new-name
cluster_B
```

5. Verify on the remote cluster that the local cluster was renamed and is running normally:

   `metrocluster node show`

   In the following example, the newly renamed `cluster_B` is running normally:

```
cluster_B::*> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   normal
              node_B_2           configured     enabled   normal
      cluster_A
              node_A_1           configured     enabled   normal
              node_A_2           configured     enabled   normal
4 entries were displayed.
```

6. Repeat these steps for each cluster that you want to rename.

Powering off and powering on a data center

You must know how to power off and power on a data center for the purpose of site maintenance or to relocate a site to another location.

If a site needs to be relocated and reconfigured (if you need to expand from a four-node to an eight-node cluster, for example), these tasks cannot be completed at the same time. This procedure only covers the steps that are required to perform site maintenance or to relocate a site without changing its configuration.

> This procedure is for use in both MetroCluster IP and FC configurations.

Powering off a MetroCluster site

You must power off a site and all of the equipment before site maintenance or relocation can begin.

Steps

1. Before you begin, check that any non-mirrored aggregates at the site are offline.
2. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:
      `node run -node *node-name* sysconfig -a`
   b. Check for any health alerts on both clusters:
      `system health alert show`
   c. Confirm the MetroCluster configuration and that the operational mode is normal:
      `metrocluster show`
   d. Perform a MetroCluster check:
      `metrocluster check run`
   e. Display the results of the MetroCluster check:
      `metrocluster check show`
   f. Check for any health alerts on the switches (if present):
      `storage switch show`
   g. Run Config Advisor.

      [NetApp Downloads: Config Advisor]
   h. After running Config Advisor, review the tool’s output and follow the recommendations in the output to address any issues discovered.
3. Enter the following command to implement the switchover:

   ```
   metrocluster switchover
   ```

   The operation can take several minutes to complete.

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.

4. Monitor and verify the completion of the switchover:

   `metrocluster operation show`

```
cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
State: in-progress
   End time: -
     Errors:

cluster_A::*> metrocluster operation show
  Operation: Switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

5. If you are in a MetroCluster IP configuration running ONTAP 9.6 or later, wait for the disaster site plexes to come online and the healing operations to automatically complete.

   In MetroCluster IP configurations running earlier versions of ONTAP, the disaster site nodes do not automatically boot to ONTAP and the plexes remain offline.

6. Depending on your configuration and ONTAP version, identify and move offline affected plexes that are located at the disaster site.

   This step is required in the following configurations:.

   - All MetroCluster FC configurations.
   - MetroCluster IP configurations running ONTAP version 9.6 or later.

   You should move the following plexes offline:

   - Non-mirrored plexes residing on disks located at the disaster site.

     If you do not move the non-mirrored plexes at the disaster site offline, an outage might result when the disaster site is later powered off.

   - Mirrored plexes residing on disks located at the disaster site for aggregate mirroring. Once they are moved offline, the plexes are inaccessible.

     a. Identify the affected plexes.

Plexes that are owned by nodes at the surviving site consist of Pool1 disks. Plexes that are owned by nodes at the disaster site consist of Pool0 disks.

> “Home” refers to the “home” owner, not the “current” owner.

```
Cluster_A::> storage aggregate plex show -fields
aggregate,status,is-online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
Node_B_1_aggr0 plex0 normal,active true     0
Node_B_1_aggr0 plex1 normal,active true     1

Node_B_2_aggr0 plex0 normal,active true     0
Node_B_2_aggr0 plex5 normal,active true     1

Node_B_1_aggr1 plex0 normal,active true     0
Node_B_1_aggr1 plex3 normal,active true     1

Node_B_2_aggr1 plex0 normal,active true     0
Node_B_2_aggr1 plex1 normal,active true     1

Node_A_1_aggr0 plex0 normal,active true     0
Node_A_1_aggr0 plex4 normal,active true     1

Node_A_1_aggr1 plex0 normal,active true     0
Node_A_1_aggr1 plex1 normal,active true     1

Node_A_2_aggr0 plex0 normal,active true     0
Node_A_2_aggr0 plex4 normal,active true     1

Node_A_2_aggr1 plex0 normal,active true     0
Node_A_2_aggr1 plex1 normal,active true     1
14 entries were displayed.

Cluster_A::>
```

The affected plexes are those that are remote to cluster A. The following table shows whether the disks are local or remote relative to cluster A:

Node	Disks in pool	Should the disks be set offline?	Example of plexes to be moved offline
Node _A_1 and Node _A_2	Disks in pool 0	No. Disks are local to cluster A.	-
	Disks in pool 1	Yes. Disks are remote to cluster A.	Node_A_1_aggr0/plex 4 Node_A_1_aggr1/plex 1 Node_A_2_aggr0/plex 4 Node_A_2_aggr1/plex 1
Node _B_1 and Node _B_2	Disks in pool 0	Yes. Disks are remote to cluster A.	Node_B_1_aggr1/plex 0 Node_B_1_aggr0/plex 0 Node_B_2_aggr0/plex 0 Node_B_2_aggr1/plex 0
	Disks in pool 1	No. Disks are local to cluster A.	-

b. Move the affected plexes offline:
`storage aggregate plex offline`

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex
plex0
```

Perform this for all plexes that have disks that are remote to Cluster_A.

7. Persistently offline the switchports according to the switch type.

This step is only required for MetroCluster FC configurations. Skip this step if your configuration is a MetroCluster IP configuration or a stretched MetroCluster configuration with FC backend switches.

Switch type	Action

If the FC switches are Brocade switches…	a. Use the **`portcfgpersistentdisable port`** command to persistently disable the ports as shown in the following example. This must be done on both switches at the surviving site.
	
	`Switch_A_1:admin>`
	`portcfgpersistentdisable 14`
	`Switch_A_1:admin>`
	`portcfgpersistentdisable 15`
	`Switch_A_1:admin>`
	
	b. Verify that the ports are disabled using the **`switchshow`** command shown in the following example:
	
	`Switch_A_1:admin> switchshow`
	`switchName:    Switch_A_1`
	`switchType:    109.1`
	`switchState:   Online`
	`switchMode:    Native`
	`switchRole:    Principal`
	`switchDomain:  2`
	`switchId:  fffc02`
	`switchWwn:`
	`10:00:00:05:33:88:9c:68`
	`zoning:        ON (T5_T6)`
	`switchBeacon:  OFF`
	`FC Router: OFF`
	`FC Router BB Fabric ID:`
	`128`
	`Address Mode:  0`
	
	`Index Port Address Media`
	`Speed State     Proto`
	
	`==============================`
	`================`
	`...`
	`14  14   020e00   id    16G`
	`No_Light    FC  Disabled`
	`(Persistent)`
	`15  15   020f00   id    16G`
	`No_Light    FC  Disabled`
	`(Persistent)`
	`...`
	`Switch_A_1:admin>`

<table>
<tr><th>Switch type</th><th>Action</th></tr>
<tr><td>If the FC switches are Cisco switches…</td><td>

a. Use the <code>interface</code> command to persistently disable the ports. The following example shows ports 14 and 15 being disabled:

```
 Switch_A_1# conf t
 Switch_A_1(config)# interface
fc1/14-15
 Switch_A_1(config)# shut

 Switch_A_1(config-if)# end
 Switch_A_1# copy running-
config startup-config
```

b. Verify that the switch port is disabled using the <code>show interface brief</code> command as shown in the following example:

```
 Switch_A_1# show interface
brief
 Switch_A_1
```

</td></tr>
</table>

8. Power off the site.

   The following equipment needs to be turned off in no specific order:

Configuration type	Equipment to be powered off
In a MetroCluster IP configuration, power off…	• MetroCluster IP switches • Storage controllers • Storage shelves
In a MetroCluster FC configuration, power off…	• MetroCluster FC switches • Storage controllers • Storage shelves • Atto FibreBridges (if present)

Relocating the powered-off site of the MetroCluster

Once the site is powered off, you can begin maintenance work. The procedure is the same whether the MetroCluster components are relocated within the same data center or relocated to a different data center.

- The hardware should be cabled in the same way as the previous site.
- If the Inter-Switch Link (ISL) speed, length, or number has changed, they all need to be reconfigured.

Steps

1. Make sure that the cabling for all components is carefully recorded so that it can be correctly reconnected at the new location.
2. Physically relocate all the hardware, storage controllers, FC and IP switches, FibreBridges, and storage shelves.
3. Configure the ISL ports and verify the intersite connectivity.
   a. Power on the FC and IP switches.

      Do **not** power up any other equipment.

4. Enable the ports.

   This step is only required in MetroCluster FC configurations. You can skip this step if your configuration is a MetroCluster IP configuration.

   Enable the ports according to the correct switch types in the following table:

Switch type	Command

If the FC Switches are Brocade switches…	a. Use the **`portcfgpersistentenable`** ***`port number`*** command to persistently enable the port. This must be done on both switches at the surviving site.
	
	The following example shows ports 14 and 15 being enabled on Switch_A_1.
	
	`switch_A_1:admin> portcfgpersistentenable 14`
	`switch_A_1:admin> portcfgpersistentenable 15`
	`switch_A_1:admin>`
	
	b. Verify that the switch port is enabled: **`switchshow`**
	
	The following example shows that ports 14 and 15 are enabled:

Switch type	Command

If the FC Switches are Cisco switches…	a. Enter the **`interface`** command to enable the port.
	
	The following example shows ports 14 and 15 being enabled on Switch_A_1.
	
	`switch_A_1# conf t`
	`switch_A_1(config)# interface fc1/14-15`
	`switch_A_1(config)# no shut`
	`switch_A_1(config-if)# end`
	`switch_A_1# copy running-config startup-config`
	
	b. Verify that the switch port is enabled: **`show interface brief`**
	
	`switch_A_1# show interface brief`
	`switch_A_1#`

```
 14  14   020e00   id    16G
Online      FC  E-Port
10:00:00:05:33:86:89:cb
"Switch_A_1"
 15  15   020f00   id    16G
Online      FC  E-Port
10:00:00:05:33:86:89:cb
"Switch_A_1" (downstream)
 ...
switch_A_1:admin>
```

5. Use tools on the switches (as they are available) to verify the intersite connectivity.

   > ⓘ You should only proceed if the links are properly configured and stable.

6. Disable the links again if they are found to be stable.

   Disable the ports based on whether you are using Brocade or Cisco switches as shown in the following table:

<table>
<tr><th>Switch type</th><th>Command</th></tr>
<tr><td>If the FC Switches are Brocade switches…</td><td>

a. Enter the **`portcfgpersistentdisable`** ***`port number`*** command to persistently disable the port.

   This must be done on both switches at the surviving site. The following example shows ports 14 and 15 being disabled on Switch_A_1:

```
 switch_A_1:admin>
portpersistentdisable 14
 switch_A_1:admin>
portpersistentdisable 15
 switch_A_1:admin>
```

b. Verify that the switch port is disabled: **`switchshow`**

   The following example shows that ports 14 and 15 are disabled:

</td></tr>
</table>

Switch type	Command

If the FC Switches are Cisco switches…	a. Disable the port using the **`interface`** command.
	
	The following example shows ports fc1/14 and fc1/15 being disabled on Switch A_1:
	
	`switch_A_1# conf t`
	
	`switch_A_1(config)# interface fc1/14-15`
	`switch_A_1(config)# shut`
	`switch_A_1(config-if)# end`
	`switch_A_1# copy running-config startup-config`
	
	b. Verify that the switch port is disabled using the **`show interface brief`** command.
	
	`switch_A_1# show interface brief`
	`switch_A_1#`

```
(Persistent)
  15  15   020f00   id    16G
No_Light    FC  Disabled
(Persistent)
...
switch_A_1:admin>
```

Powering on the MetroCluster configuration and returning to normal operation

After maintenance has been completed or the site has been moved, you must power on the site and reestablish the MetroCluster configuration.

Steps

1. Power on the switches.

   Switches should be powered on first. They might have been powered on during the previous step if the site was relocated.

   a. Reconfigure the Inter-Switch Link (ISL) if required or if this was not completed as part of the relocation.

   b. Enable the ISL if fencing was completed.

   c. Verify the ISL.

2. Power on the shelves and allow enough time for them to power on completely.

3. Power on the FibreBridge bridges.

   > You can skip this step if your configuration is a MetroCluster IP configuration.

   a. On the FC switches, verify that the ports connecting the bridges are coming online.

You can use a command such as **`switchshow`** for Brocade switches, and **`show interface brief`** for Cisco switches.

b. Verify that the shelves and disks on the bridges are clearly visible.

You can use a command such as **`sastargets`** on the ATTO command-line interface (CLI).

4. Enable the ISLs on the FC switches.

> Skip this step if your configuration is a MetroCluster IP configuration.

Enable the ports based on whether you are using Brocade or Cisco switches as shown in the following table:

<table>
<tr><th>Switch type</th><th>Command</th></tr>
<tr><td>If the FC Switches are Brocade switches…</td><td>

a. Enter the <code>portcfgpersistentenable port</code> command to persistently enable the ports. This must be done on both switches at the surviving site.

The following example shows ports 14 and 15 being enabled on Switch_A_1:

```
 Switch_A_1:admin>
portcfgpersistentenable 14
 Switch_A_1:admin>
portcfgpersistentenable 15
 Switch_A_1:admin>
```

b. Verify that the switch port is enabled using the <code>switchshow</code> command:

</td></tr>
</table>

Switch type	Command

If the FC Switches are Cisco switches…	a. Use the **`interface`** command to enable the ports.
	
	The following example shows port fc1/14 and fc1/15 being enabled on Switch A_1:
	
	`switch_A_1# conf t`
	`switch_A_1(config)# interface fc1/14-15`
	`switch_A_1(config)# no shut`
	`switch_A_1(config-if)# end`
	`switch_A_1# copy running-config startup-config`
	
	b. Verify that the switch port is disabled:
	
	`switch_A_1# show interface brief`
	`switch_A_1#`

```
================
   ...
   14  14   020e00   id    16G
Online      FC  E-Port
10:00:00:05:33:86:89:cb
```

5. Verify that the storage is now visible.

   Select the appropriate method of determining whether the storage is visible based on whether you have a MetroCluster IP or FC configuration:

Configuration	Step
If your configuration is a MetroCluster IP…	Verify that the local storage is visible from the node Maintenance mode.
If your configuration is a MetroCluster FC…	Verify that the storage is visible from the surviving site. Put the offline plexes back online. This restarts the resync operations and reestablishes the SyncMirror.

6. Reestablish the MetroCluster configuration.

   Follow the instructions in the *MetroCluster Disaster and Recovery Guide* to perform healing and switchback operations according to your MetroCluster configuration.

   MetroCluster management and disaster recovery

Powering off an entire MetroCluster IP configuration

You must power off the entire MetroCluster IP configuration and all of the equipment before maintenance or relocation can begin.

> Starting with ONTAP 9.8, the **storage switch** command is replaced with **system switch**. The following steps show the **storage switch** command, but if you are running ONTAP 9.8 or later, the **system switch** command is preferred.

1. Verify the MetroCluster configuration from both sites in the MetroCluster configuration.
   a. Confirm that the MetroCluster configuration and operational mode are normal.
      metrocluster show
   b. Run the following command:
      metrocluster interconnect show
   c. Confirm connectivity to the disks by entering the following command on any one of the MetroCluster nodes:
      run local sysconfig -v
   d. Run the following command:
      storage port show
   e. Run the following command:
      storage switch show
   f. Run the following command:
      network interface show
   g. Run the following command:
      network port show
   h. Run the following command:
      network device-discovery show
   i. Perform a MetroCluster check:
      metrocluster check run
   j. Display the results of the MetroCluster check:
      metrocluster check show
   k. Run the following command:
      metrocluster configuration-settings interface show
2. If necessary, disable AUSO by modifying the AUSO Failure Domain to

   auso-disabled

   ```
   cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
   auso-disabled
   ```

   > In a MetroCluster IP configuration, the AUSO Failure Domain is already set to 'auso-disabled' unless the configuration is configured with ONTAP Mediator.

3. Verify the change using the command

   `metrocluster operation show`

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. Halt the nodes:

   `halt`

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

5. Power off the following equipment at the site:
   - Storage controllers
   - MetroCluster IP switches
   - Storage shelves
6. Wait for thirty minutes and then power on all the controllers.
7. After the controllers are powered on, verify the MetroCluster configuration from both sites.

   To verify the configuration, repeat step 1.

8. Perform power cycle checks.
   a. Verify that all sync-source SVMs are online:
      `vserver show`
   b. Start any sync-source SVMs that are not online:
      `vserver start`

Powering off an entire MetroCluster FC configuration

You must power off the entire MetroCluster FC configuration and all of the equipment before site maintenance or relocation can begin.

> Starting with ONTAP 9.8, the **`storage switch`** command is replaced with **`system switch`**. The following steps show the **`storage switch`** command, but if you are running ONTAP 9.8 or later, the **`system switch`** command is preferred.

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

a. Confirm the MetroCluster configuration and that the operational mode is normal.
   metrocluster show
b. Confirm connectivity to the disks by entering the following command on any one of the MetroCluster nodes:
   run local sysconfig -v
c. Run the following command:
   storage bridge show
d. Run the following command:
   storage port show
e. Run the following command:
   storage switch show
f. Run the following command:
   network port show
g. Perform a MetroCluster check:
   metrocluster check run
h. Display the results of the MetroCluster check:
   metrocluster check show

2. Disable AUSO by modifying the AUSO Failure Domain to

   auso-disabled

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```

3. Verify the change using the command

   metrocluster operation show

```
    cluster_A_site_A::*> metrocluster operation show
       Operation: modify
           State: successful
      Start Time: 4/25/2020 20:20:36
        End Time: 4/25/2020 20:20:36
          Errors: -
```

4. Halt the nodes by using the following command:

   halt * For a four-node or eight-node MetroCluster configuration, use the parameter *inhibit-takeover

   +

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

◦ For a two-node MetroCluster configuration, use the command:

```
system node halt -node node1_SiteA -ignore-quorum-warnings true
```

5. Power off the following equipment at the site:
   ◦ Storage controllers
   ◦ MetroCluster FC switches
   ◦ ATTO FibreBridges
   ◦ Storage shelves
6. Wait for thirty minutes and then power on all the controllers.
7. After the controllers are powered on, verify the MetroCluster configuration from both sites.

   To verify the configuration, repeat step 1.

8. Perform power cycle checks.
   a. Verify that all sync-source SVMs are online:
      `vserver show`
   b. Start any sync-source SVMs that are not online:
      `vserver start`

Reconfiguring an FC switch layout configured before ONTAP 9.x

If your existing FC switch layout was configured prior to ONTAP 9.1, you must reconfigure the port layout and apply the latest Reference Configuration Files (RCFs). This procedure applies only to MetroCluster FC configurations.

You must identify the FC switches present in the fabric domain.

You need the admin password and access to an FTP or SCP server.

You must perform this task if your existing FC switch layout was configured prior to ONTAP 9.1. It is *not* required if you are upgrading from an existing switch layout that was configured for ONTAP 9.1 or later.

This procedure is nondisruptive and takes approximately four hours to complete (excluding rack and stack) when disks are zeroed.

Sending a custom AutoSupport message prior to reconfiguring switches

Before reconfiguring your switches, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster.
2. Invoke an AutoSupport message indicating the start of the maintenance:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*`*`

   maintenance-window-in-hours specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Repeat these steps on the partner site.

Verifying the health of the MetroCluster configuration

You should check the health of the MetroCluster configuration to verify proper operation.

Steps

1. Verify that the MetroCluster components are healthy:

   `metrocluster check run`

   ```
   cluster_A::*> metrocluster check run
   ```

   The operation runs in the background.

2. After the `metrocluster check run` operation completes, run `metrocluster check show` to view the results.

   After approximately five minutes, the following results are displayed:

```
-----------
cluster_A::*> metrocluster check show

Last Checked On: 4/7/2019 21:15:05

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          warning
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

3. To check the status of the running MetroCluster check operation, use the command:

   `metrocluster operation history show -job-id 38`

4. Verify that there are no health alerts:

   `system health alert show`

Checking for MetroCluster configuration errors

You can use the Config Advisor tool available from the NetApp Support Site to check for common configuration errors.

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.

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

1. Download the Config Advisor tool.

   NetApp Downloads: Config Advisor

2. Run Config Advisor, reviewing the output and following its recommendations to address any issues.

Persistently disabling the switches

You must disable the switches in the fabric persistently so that you can modify its configuration.

You disable the switches by running the commands on the switch command line; the commands used for this are not ONTAP commands.

Steps

1. Persistently disable the switch:
   - For Brocade switches, use the `switchCfgPersistentDisable` command.
   - For Cisco switches, use the `suspend` command. The following command disables a Brocade switch persistently:

     ```
     FC_switch_A_1:admin> switchCfgPersistentDisable
     ```

     The following command disables a Cisco switch:

     ```
     vsan [vsna #] suspend
     ```

Determining the new cabling layout

You must determine the cabling for the new controller modules and any new disk shelves to the existing FC switches.

This task must be performed at each MetroCluster site.

Steps

1. Use the *Fabric-attached MetroCluster Installation and Configuration Guide* to determine the cabling layout for your switch type, using the port usage for an eight-node MetroCluster configuration.

   The FC switch port usage must match the usage described in the guide so that the Reference Configuration Files (RCFs) can be used.

   Fabric-attached MetroCluster installation and configuration

   > ⓘ If your environment cannot be cabled in a way that RCFs can be used, then contact technical support. Do not use this procedure if the cabling cannot use RCFs.

Applying RCF files and recabling the switches

You must apply the appropriate reference configuration (RCF) files to reconfigure your switches to accommodate the new nodes. After you apply the RCF files, you can recable the switches.

The FC switch port usage must match the usage described in the *Fabric-attached MetroCluster Installation and Configuration Guide* so that the RCFs can be used.

Fabric-attached MetroCluster installation and configuration

Steps

1. Locate the RCF files for your configuration.

   You must use the RCF files that match your switch model.

2. Apply the RCF files, following the directions on the Download page and adjusting the ISL settings as needed.
3. Verify that the switch configuration is saved.
4. Cable both of the FC-to-SAS bridges to the FC switches, using the cabling layout you created in the “Determining the new cabling layout” section.
5. Verify that the ports are online:
   - For Brocade switches, use the `switchshow` command.
   - For Cisco switches, use the `show interface brief` command.
6. Cable the FC-VI ports from the controllers to the switches.
7. From the existing nodes, verify that the FC-VI ports are online:

   `metrocluster interconnect adapter show`

   `metrocluster interconnect mirror show`

Persistently enable the switches

You must enable the switches in the fabric persistently.

Steps

1. Persistently enable the switch:
   - For Brocade switches, use the `switchCfgPersistentenable` command.
   - For Cisco switches, use the no `suspend` command. The following command persistently enables a Brocade switch:

     ```
     FC_switch_A_1:admin> switchCfgPersistentenable
     ```

     The following command enables a Cisco switch:

     ```
     vsan [vsna #]no suspend
     ```

Verifying switchover, healing, and switchback

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

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

Port assignments for FC switches

You need to verify that you are using the specified port assignments when you cable the FC switches. The port assignments are different between ONTAP 9.0 and later versions of ONTAP.

Port assignments for systems using two initiator ports

You can configure FAS8020, AFF8020, FAS8200, and AFF A300 systems using a single initiator port for each fabric and two initiator ports for each controller.

You can follow the cabling for the FibreBridge 6500N bridge or FibreBridge 7500N or 7600N bridge using only one FC port (FC1 or FC2). Instead of using four initiators, connect only two initiators and leave the other two that are connected to the switch port empty.

You must apply the correct RCF file for the FibreBridge 6500N bridge’s configuration.

If zoning is performed manually, then follow the zoning used for a FibreBridge 6500N or a FibreBridge 7500N or 7600N bridge using one FC port (FC1 or FC2). In this scenario, one initiator port rather than two is added to each zone member per fabric.

You can change the zoning or perform an upgrade from a FibreBridge 6500 to a FibreBridge 7500 using the procedure *Hot-swapping a FibreBridge 6500N bridge with a FibreBridge 7500N or 7600N bridge* from the MetroCluster Maintenance Guide.

The following table shows port assignments for FC switches when using ONTAP 9.1 and later.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only			
MetroCluster 1 or DR Group 1			
Component	Port	Brocade switch models 6505, 6510, 6520, 7840, G620, G610, and DCX 8510-8	
		Connects to FC switch…	Connects to switch port…

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only			
controller_x_1	FC-VI port a	1	0
	FC-VI port b	2	0
	FC-VI port c	1	1
	FC-VI port d	2	1
	HBA port a	1	2
	HBA port b	2	2
	HBA port c	-	-
	HBA port d	-	-
Stack 1	bridge_x_1a	1	8
	bridge_x_1b	2	8
Stack y	bridge_x_ya	1	11
	bridge_x_yb	2	11

The following table shows port assignments for FC switches when using ONTAP 9.0.

MetroCluster two-node configuration			
Component	Port	Brocade 6505, 6510, or DCX 8510-8	
		FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	0	-
	FC-VI port b	-	0
	HBA port a	1	-
	HBA port b	-	1
	HBA port c	2	-
	HBA port d	-	2

Port assignments for FC switches when using ONTAP 9.0

You need to verify that you are using the specified port assignments when you cable the FC switches. The port assignments are different between ONTAP 9.0 and later versions of ONTAP.

Ports that are not used for attaching initiator ports, FC-VI ports, or ISLs can be reconfigured to act as storage ports. However, if the supported RCFs are being used, the zoning must be changed accordingly.

If the supported RCF files are used, ISL ports may not connect to the same ports shown here and may need to be reconfigured manually.

Overall cabling guidelines

You should be aware of the following guidelines when using the cabling tables:

- The Brocade and Cisco switches use different port numbering:
  - On Brocade switches, the first port is numbered 0.
  - On Cisco switches, the first port is numbered 1.
- The cabling is the same for each FC switch in the switch fabric.
- AFF A300 and FAS8200 storage systems 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.

Brocade port usage for controller connections in an eight-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Brocade models Brocade 6505, 6510, or DCX 8510-8:

Component	Port	FC_switch_x_1	FC_switch_x_2
controller_x_3	FC-VI port a	6	-
controller_x_3	FC-VI port b	-	6
controller_x_3	HBA port a	7	-
controller_x_3	HBA port b	-	7
controller_x_3	HBA port c	8	-
controller_x_3	HBA port d	-	8
controller_x_4	FC-VI port a	9	-
controller_x_4	FC-VI port b	-	9
controller_x_4	HBA port a	10	-
controller_x_4	HBA port b	-	10
controller_x_4	HBA port c	11	-
controller_x_4	HBA port d	-	11

Brocade port usage for FC-to-SAS bridge connections in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage when using FibreBridge 7500 bridges:

Bridge	Bridge port	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	12	-
bridge_x_1a	FC2	-	12
bridge_x_1b	FC1	13	-
bridge_x_1b	FC2	-	13
bridge_x_2a	FC1	14	-
bridge_x_2a	FC2	-	14
bridge_x_2b	FC1	15	-
bridge_x_2b	FC2	-	15
bridge_x_3a	FC1	16	-
bridge_x_3a	FC2	-	16
bridge_x_3b	FC1	17	-
bridge_x_3b	FC2	-	17
bridge_x_4a	FC1	18	-
bridge_x_4a	FC2	-	18
bridge_x_4b	FC1	19	-
bridge_x_4b	FC2	-	19

The following table shows bridge port usage when using FibreBridge 6500 bridges with Brocade 6505, 6510, or DCX 8510-8 switches:

Bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	12	-
bridge_x_1b	FC1	-	12
bridge_x_2a	FC1	13	-
bridge_x_2b	FC1	-	13
bridge_x_3a	FC1	14	-
bridge_x_3b	FC1	-	14
bridge_x_4a	FC1	15	-
bridge_x_4b	FC1	-	15
bridge_x_5a	FC1	16	-
bridge_x_5b	FC1	-	16
bridge_x_6a	FC1	17	-

Bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_6b	FC1	-	17
bridge_x_7a	FC1	18	-
bridge_x_7b	FC1	-	18
bridge_x_8a	FC1	19	-
bridge_x_8b	FC1	-	19

Brocade port usage for ISLs in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage for Brocade 6505, 6510, or DCX 8510-8 switches:

ISL port	FC_switch_x_1	FC_switch_x_2
ISL port 1	20	20
ISL port 2	21	21
ISL port 3	22	22
ISL port 4	23	23

Brocade port usage for controllers in a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric. The following table shows usage for the Brocade 6505, 6510, and DCX 8510-8 switches.

Component	Port	FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	0	-
controller_x_1	FC-VI port b	-	0
controller_x_1	HBA port a	1	-
controller_x_1	HBA port b	-	1
controller_x_1	HBA port c	2	-
controller_x_1	HBA port d	-	2
controller_x_2	FC-VI port a	3	-
controller_x_2	FC-VI port b	-	3
controller_x_2	HBA port a	4	-
controller_x_2	HBA port b	-	4
controller_x_2	HBA port c	5	-
controller_x_2	HBA port d	-	5

Brocade port usage for bridges in a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows bridge port usage up to port 17 when using FibreBridge 7500 bridges. Additional bridges can be cabled to ports 18 through 23.

FibreBridge 7500 bridge	Port	FC_switch_x_1 (6510 or DCX 8510-8)	FC_switch_x_2 (6510 or DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
bridge_x_1a	FC1	6	-	6	-
bridge_x_1a	FC2	-	6	-	6
bridge_x_1b	FC1	7	-	7	-
bridge_x_1b	FC2	-	7	-	7
bridge_x_2a	FC1	8	-	12	-
bridge_x_2a	FC2	-	8	-	12
bridge_x_2b	FC1	9	-	13	-
bridge_x_2b	FC2	-	9	-	13
bridge_x_3a	FC1	10	-	14	-
bridge_x_3a	FC2	-	10	-	14
bridge_x_3b	FC1	11	-	15	-
bridge_x_3b	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
bridge_x_4a	FC2	-	12	-	16
bridge_x_4b	FC1	13	-	17	-
bridge_x_4b	FC2	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47			

The following table shows bridge port usage when using FibreBridge 6500 bridges:

	6500N bridge port	FC_switch_x_1 (6510 or DCX 8510-8)	FC_switch_x_2 (6510 or DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
bridge_x_1a	FC1	6	-	6	-
bridge_x_1b	FC1	-	6	-	6
bridge_x_2a	FC1	7	-	7	-
bridge_x_2b	FC1	-	7	-	7
bridge_x_3a	FC1	8	-	12	-
bridge_x_3b	FC1	-	8	-	12

	6500N bridge port	FC_switch_x_1 (6510 or DCX 8510-8)	FC_switch_x_2 (6510 or DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
bridge_x_4a	FC1	9	-	13	-
bridge_x_4b	FC1	-	9	-	13
bridge_x_5a	FC1	10	-	14	-
bridge_x_5b	FC1	-	10	-	14
bridge_x_6a	FC1	11	-	15	-
bridge_x_6b	FC1	-	11	-	15
bridge_x_7a	FC1	12	-	16	-
bridge_x_7b	FC1	-	12	-	16
bridge_x_8a	FC1	13	-	17	-
bridge_x_8b	FC1	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

Brocade port usage for ISLs in a four-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage:

ISL port	FC_switch_x_1 (6510 or DCX 8510-8)	FC_switch_x_2 (6510 or DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
ISL port 1	20	20	8	8
ISL port 2	21	21	9	9
ISL port 3	22	22	10	10
ISL port 4	23	23	11	11

Brocade port usage for controllers in a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric. The following table shows the cabling for Brocade 6505, 6510, and DCX 8510-8 switches.

Component	Port	FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	0	-
controller_x_1	FC-VI port b	-	0
controller_x_1	HBA port a	1	-
controller_x_1	HBA port b	-	1

Component	Port	FC_switch_x_1	FC_switch_x_2
controller_x_1	HBA port c	2	-
controller_x_1	HBA port d	-	2

Brocade port usage for bridges in a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows bridge port usage up to port 17 when using FibreBridge 7500 bridges with Brocade 6505, 6510, and DCX 8510-8 switches. Additional bridges can be cabled to ports 18 through 23.

FibreBridge 7500 bridge	Port	FC_switch_x_1 (6510 or DCX 8510-8)	FC_switch_x_2 (6510 or DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
bridge_x_1a	FC1	6	-	6	-
bridge_x_1a	FC2	-	6	-	6
bridge_x_1b	FC1	7	-	7	-
bridge_x_1b	FC2	-	7	-	7
bridge_x_2a	FC1	8	-	12	-
bridge_x_2a	FC2	-	8	-	12
bridge_x_2b	FC1	9	-	13	-
bridge_x_2b	FC2	-	9	-	13
bridge_x_3a	FC1	10	-	14	-
bridge_x_3a	FC2	-	10	-	14
bridge_x_3a	FC1	11	-	15	-
bridge_x_3a	FC2	-	11	-	15
bridge_x_4a	FC1	12	-	16	-
bridge_x_4a	FC2	-	12	-	16
bridge_x_4b	FC1	13	-	17	-
bridge_x_4b	FC2	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

The following table shows bridge port usage when using FibreBridge 6500 bridges with Brocade 6505, 6510, and DCX 8510-8 switches:

FibreBridge 6500 bridge	Port	FC_switch_x_1 (6510 or DCX 8510-8)	FC_switch_x_2 (6510 or DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
bridge_x_1a	FC1	6	-	6	-
bridge_x_1b	FC1	-	6	-	6
bridge_x_2a	FC1	7	-	7	-
bridge_x_2b	FC1	-	7	-	7
bridge_x_3a	FC1	8	-	12	-
bridge_x_3b	FC1	-	8	-	12
bridge_x_4a	FC1	9	-	13	-
bridge_x_4b	FC1	-	9	-	13
bridge_x_5a	FC1	10	-	14	-
bridge_x_5b	FC1	-	10	-	14
bridge_x_6a	FC1	11	-	15	-
bridge_x_6b	FC1	-	11	-	15
bridge_x_7a	FC1	12	-	16	-
bridge_x_7b	FC1	-	12	-	16
bridge_x_8a	FC1	13	-	17	-
bridge_x_8b	FC1	-	13	-	17
		additional bridges can be cabled through port 19, then ports 24 through 47		additional bridges can be cabled through port 23	

Brocade port usage for ISLs in a two-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage for Brocade 6505, 6510, and DCX 8510-8 switches:

ISL port	FC_switch_x_1 (6510 or DCX 8510-8)	FC_switch_x_2 (6510 or DCX 8510-8)	FC_switch_x_1 (6505)	FC_switch_x_2 (6505)
ISL port 1	20	20	8	8
ISL port 2	21	21	9	9
ISL port 3	22	22	10	10
ISL port 4	23	23	11	11

Cisco port usage for controllers in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows controller port usage on Cisco 9148 and 9148S switches:

Component	Port	FC_switch_x_1	FC_switch_x_2
controller_x_3	FC-VI port a	7	-
controller_x_3	FC-VI port b	-	7
controller_x_3	HBA port a	8	-
controller_x_3	HBA port b	-	8
controller_x_3	HBA port c	9	-
controller_x_3	HBA port d	-	9
controller_x_4	FC-VI port a	10	-
controller_x_4	FC-VI port b	-	10
controller_x_4	HBA port a	11	-
controller_x_4	HBA port b	-	11
controller_x_4	HBA port c	13	-
controller_x_4	HBA port d	-	13

Cisco port usage for FC-to-SAS bridges in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage up to port 23 when using FibreBridge 7500 bridges when using Cisco 9148 or 9148S switches. Additional bridges can be attached using ports 25 through 48.

FibreBridge 7500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	14	14
bridge_x_1a	FC2	-	-
bridge_x_1b	FC1	15	15
bridge_x_1b	FC2	-	-
bridge_x_2a	FC1	17	17
bridge_x_2a	FC2	-	-
bridge_x_2b	FC1	18	18
bridge_x_2b	FC2	-	-
bridge_x_3a	FC1	19	19
bridge_x_3a	FC2	-	-
bridge_x_3b	FC1	21	21
bridge_x_3b	FC2	-	-
bridge_x_4a	FC1	22	22

FibreBridge 7500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_4a	FC2	-	-
bridge_x_4b	FC1	23	23
bridge_x_4b	FC2	-	-

Additional bridges can be attached using ports 25 through 48 following the same pattern.

The following table shows bridge port usage up to port 23 when using FibreBridge 6500 bridges with Cisco 9148 or 9148S switches. Additional bridges can be attached using ports 25-48.

FibreBridge 6500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	14	-
bridge_x_1b	FC1	-	14
bridge_x_2a	FC1	15	-
bridge_x_2b	FC1	-	15
bridge_x_3a	FC1	17	-
bridge_x_3b	FC1	-	17
bridge_x_4a	FC1	18	-
bridge_x_4b	FC1	-	18
bridge_x_5a	FC1	19	-
bridge_x_5b	FC1	-	19
bridge_x_6a	FC1	21	-
bridge_x_6b	FC1	-	21
bridge_x_7a	FC1	22	-
bridge_x_7b	FC1	-	22
bridge_x_8a	FC1	23	-
bridge_x_8b	FC1	-	23

Additional bridges can be attached using ports 25 through 48 following the same pattern.

Cisco port usage for ISLs in an eight-node MetroCluster configuration running ONTAP 9.0

The following table shows ISL port usage for Cisco 9148 and 9148S switches:

ISL ports	FC_switch_x_1	FC_switch_x_2
ISL port 1	12	12
ISL port 2	16	16
ISL port 3	20	20
ISL port 4	24	24

Cisco port usage for controllers in a four-node MetroCluster configuration

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Cisco 9148, 9148S, and 9250i switches:

Component	Port	FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	1	-
controller_x_1	FC-VI port b	-	1
controller_x_1	HBA port a	2	-
controller_x_1	HBA port b	-	2
controller_x_1	HBA port c	3	-
controller_x_1	HBA port d	-	3
controller_x_2	FC-VI port a	4	-
controller_x_2	FC-VI port b	-	4
controller_x_2	HBA port a	5	-
controller_x_2	HBA port b	-	5
controller_x_2	HBA port c	6	-
controller_x_2	HBA port d	-	6

Cisco port usage for FC-to-SAS bridges in a four-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage up to port 14 when using FibreBridge 7500 bridges with Cisco 9148, 9148S, or 9250i switches. Additional bridges can be attached to ports 15 through 32 following the same pattern.

FibreBridge 7500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
bridge_x_1a	FC2	-	7
bridge_x_1b	FC1	8	-
bridge_x_1b	FC2	-	8
bridge_x_2a	FC1	9	-
bridge_x_2a	FC2	-	9
bridge_x_2b	FC1	10	-
bridge_x_2b	FC2	-	10
bridge_x_3a	FC1	11	-
bridge_x_3a	FC2	-	11
bridge_x_3b	FC1	12	-
bridge_x_3b	FC2	-	12

FibreBridge 7500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_4a	FC1	13	-
bridge_x_4a	FC2	-	13
bridge_x_4b	FC1	14	-
bridge_x_4b	FC2	-	14

The following table shows bridge port usage when using FibreBridge 6500 bridges up to port 14 on Cisco 9148, 9148S, or 9250i switches. Additional bridges can be attached to ports 15 through 32 following the same pattern.

FibreBridge 6500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
bridge_x_1b	FC1	-	7
bridge_x_2a	FC1	8	-
bridge_x_2b	FC1	-	8
bridge_x_3a	FC1	9	-
bridge_x_3b	FC1	-	9
bridge_x_4a	FC1	10	-
bridge_x_4b	FC1	-	10
bridge_x_5a	FC1	11	-
bridge_x_5b	FC1	-	11
bridge_x_6a	FC1	12	-
bridge_x_6b	FC1	-	12
bridge_x_7a	FC1	13	-
bridge_x_7b	FC1	-	13
bridge_x_8a	FC1	14	-
bridge_x_8b	FC1	-	14

Additional bridges can be attached to ports 15 through 32 following the same pattern.

Cisco 9148 and 9148S port usage for ISLs on a four-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows ISL port usage for Cisco 9148 and 9148S switches:

ISL port	FC_switch_x_1	FC_switch_x_2
ISL port 1	36	36
ISL port 2	40	40

ISL port	FC_switch_x_1	FC_switch_x_2
ISL port 3	44	44
ISL port 4	48	48

Cisco 9250i port usage for ISLs on a four-node MetroCluster configuration running ONTAP 9.0

The Cisco 9250i switch uses the FCIP ports for the ISL.

Ports 40 through 48 are 10 GbE ports and are not used in the MetroCluster configuration.

Cisco port usage for controllers in a two-node MetroCluster configuration

The cabling is the same for each FC switch in the switch fabric.

The following table shows controller port usage on Cisco 9148, 9148S, and 9250i switches:

Component	Port	FC_switch_x_1	FC_switch_x_2
controller_x_1	FC-VI port a	1	-
controller_x_1	FC-VI port b	-	1
controller_x_1	HBA port a	2	-
controller_x_1	HBA port b	-	2
controller_x_1	HBA port c	3	-
controller_x_1	HBA port d	-	3

Cisco port usage for FC-to-SAS bridges in a two-node MetroCluster configuration running ONTAP 9.0

The following table shows bridge port usage up to port 14 when using FibreBridge 7500 bridges with Cisco 9148, 9148S, and 9250i switches. Additional bridges can be attached to ports 15 through 32 following the same pattern.

FibreBridge 7500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
bridge_x_1a	FC2	-	7
bridge_x_1b	FC1	8	-
bridge_x_1b	FC2	-	8
bridge_x_2a	FC1	9	-
bridge_x_2a	FC2	-	9
bridge_x_2b	FC1	10	-
bridge_x_2b	FC2	-	10
bridge_x_3a	FC1	11	-
bridge_x_3a	FC2	-	11
bridge_x_3b	FC1	12	-

FibreBridge 7500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_3b	FC2	-	12
bridge_x_4a	FC1	13	-
bridge_x_4a	FC2	-	13
bridge_x_4b	FC1	14	-
bridge_x_4b	FC2	-	14

The following table shows bridge port usage when using FibreBridge 6500 bridges up to port 14 on Cisco 9148, 9148S, or 9250i switches. Additional bridges can be attached to ports 15 through 32 following the same pattern.

FibreBridge 6500 bridge	Port	FC_switch_x_1	FC_switch_x_2
bridge_x_1a	FC1	7	-
bridge_x_1b	FC1	-	7
bridge_x_2a	FC1	8	-
bridge_x_2b	FC1	-	8
bridge_x_3a	FC1	9	-
bridge_x_3b	FC1	-	9
bridge_x_4a	FC1	10	-
bridge_x_4b	FC1	-	10
bridge_x_5a	FC1	11	-
bridge_x_5b	FC1	-	11
bridge_x_6a	FC1	12	-
bridge_x_6b	FC1	-	12
bridge_x_7a	FC1	13	-
bridge_x_7b	FC1	-	13
bridge_x_8a	FC1	14	-
bridge_x_8b	FC1	-	14

Additional bridges can be attached to ports 15 through 32 following the same pattern.

Cisco 9148 or 9148S port usage for ISLs on a two-node MetroCluster configuration running ONTAP 9.0

The cabling is the same for each FC switch in the switch fabric.

The following table shows ISL port usage for Cisco 9148 or 9148S switches:

ISL port	FC_switch_x_1	FC_switch_x_2
ISL port 1	36	36

ISL port	FC_switch_x_1	FC_switch_x_2
ISL port 2	40	40
ISL port 3	44	44
ISL port 4	48	48

Cisco 9250i port usage for ISLs on a two-node MetroCluster configuration running ONTAP 9.0

The Cisco 9250i switch uses the FCIP ports for the ISL.

Ports 40 through 48 are 10 GbE ports and are not used in the MetroCluster configuration.

Port assignments for FC switches when using ONTAP 9.1 or later

You need to verify that you are using the specified port assignments when you cable the FC switches when using ONTAP 9.1 and later.

Ports that are not used for attaching initiator ports, FC-VI ports, or ISLs can be reconfigured to act as storage ports. However, if the supported RCFs are being used, the zoning must be changed accordingly.

If the supported RCFs are used, ISL ports might not connect to the same ports shown and might need to be reconfigured manually.

If you configured your switches using the port assignments for ONTAP 9, you can continue to use the older assignments. However, new configurations running ONTAP 9.1 or later releases should use the port assignments shown here.

Overall cabling guidelines

You should be aware of the following guidelines when using the cabling tables:

- The Brocade and Cisco switches use different port numbering:
  - On Brocade switches, the first port is numbered 0.
  - On Cisco switches, the first port is numbered 1.
- The cabling is the same for each FC switch in the switch fabric.
- AFF A300 and FAS8200 storage systems 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 require four FC-VI ports. The following tables show cabling for the FC switches with four FC-VI ports on each controller except for the Cisco 9250i switch.

  For other storage systems, use the cabling shown in the tables but ignore the cabling for FC-VI ports c and d.

  You can leave those ports empty.
- AFF A400 and FAS8300 storage systems use ports 2a and 2b for FC-VI connectivity.
- If you have two MetroCluster configurations sharing ISLs, use the same port assignments as that for an eight-node MetroCluster cabling.

The number of ISLs you cable may vary depending on site’s requirements.

See the section on ISL considerations.

Brocade port usage for controllers in a MetroCluster configuration running ONTAP 9.1 or later

The following tables show port usage on Brocade switches. The tables show the maximum supported configuration, with eight controller modules in two DR groups. For smaller configurations, ignore the rows for the additional controller modules. Note that eight ISLs are supported only on the Brocade 6510, Brocade DCX 8510-8, G620, G630, G620-1, G630-1, and G720 switches.

- Port usage for the Brocade 6505 and Brocade G610 switches in an eight-node MetroCluster configuration is not shown. Due to the limited number of ports, port assignments must be made on a site-by-site basis depending on the controller module model and the number of ISLs and bridge pairs in use.
- The Brocade DCX 8510-8 switch can use the same port layout as the 6510 switch ***or*** the 7840 switch.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only				
MetroCluster 1 or DR Group 1				
Component	**Port**	**Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 and DCX 8510-8**		**Brocade switch model G720**
		Connects to FC switch…	**Connects to switch port…**	**Connects to switch port…**
controller_x_1	FC-VI port a	1	0	0
	FC-VI port b	2	0	0
	FC-VI port c	1	1	1
	FC-VI port d	2	1	1
	HBA port a	1	2	8
	HBA port b	2	2	8
	HBA port c	1	3	9
	HBA port d	2	3	9

controller_x_2	FC-VI port a	1	4	4
	FC-VI port b	2	4	4
	FC-VI port c	1	5	5
	FC-VI port d	2	5	5
	HBA port a	1	6	12
	HBA port b	2	6	12
	HBA port c	1	7	13
	HBA port d	2	7	13

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only				
MetroCluster 1 or DR Group 1				
Component	**Port**	**Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1 and DCX 8510-8**		**Brocade switch model G720**
		Connects to FC switch…	**Connects to switch port…**	**Connects to switch port…**
Stack 1	bridge_x_1a	1	8	10
	bridge_x_1b	2	8	10
Stack 2	bridge_x_2a	1	9	11
	bridge_x_2b	2	9	11
Stack 3	bridge_x_3a	1	10	14
	bridge_x_4b	2	10	14
Stack y	bridge_x_ya	1	11	15
	bridge_x_yb	2	11	15

- On G620, G630, G620-1 and G630-1 switches, additional bridges can be cabled to ports 12 - 17, 20 and 21.
- On G610 switches, additional bridges can be cabled to ports 12 - 19.
- On G720 switches, additional bridges can be cabled to ports 16 - 17, 20 and 21.

Configurations using FibreBridge 6500N bridges or FibreBridge 7500N or 7600N using one FC port (FC1 or FC2) only							
MetroCluster 2 or DR Group 2							
			Brocade switch model				
Component	**Port**	**Connects to FC_switch …**	**6510, DCX 8510-8**	**6520**	**7840, DCX 8510-8**	**G620, G620-1, G630, G630-1**	**G720**
controller_x_3	FC-VI port a	1	24	48	12	18	18
	FC-VI port b	2	24	48	12	18	18
	FC-VI port c	1	25	49	13	19	19
	FC-VI port d	2	25	49	13	19	19
	HBA port a	1	26	50	14	24	26
	HBA port b	2	26	50	14	24	26
	HBA port c	1	27	51	15	25	27
	HBA port d	2	27	51	15	25	27

controller_x_4	FC-VI port a	1	28	52	16	22	22
	FC-VI port b	2	28	52	16	22	22
	FC-VI port c	1	29	53	17	23	23
	FC-VI port d	2	29	53	17	23	23
	HBA port a	1	30	54	18	28	30
	HBA port b	2	30	54	18	28	30
	HBA port c	1	31	55	19	29	31
	HBA port d	2	32	55	19	29	31
Stack 1	bridge_x_51a	1	32	56	20	26	32
	bridge_x_51b	2	32	56	20	26	32
Stack 2	bridge_x_52a	1	33	57	21	27	33
	bridge_x_52b	2	33	57	21	27	33
Stack 3	bridge_x_53a	1	34	58	22	30	34
	bridge_x_54b	2	34	58	22	30	34
Stack y	bridge_x_ya	1	35	59	23	31	35
	bridge_x_yb	2	35	59	23	31	35

- On G720 switches, additional bridges can be cabled to ports 36-39.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)
MetroCluster 1 or DR Group 1

Component		Port	Brocade switch models 6505, 6510, 6520, 7810, 7840, G610, G620, G620-1, G630, G630-1, and DCX 8510-8		Brocade switch G720
			Connects to FC_switch…	**Connects to switch port…**	**Connects to switch port…**
Stack 1	bridge_x_1a	FC1	1	8	10
		FC2	2	8	10
	bridge_x_1B	FC1	1	9	11
		FC2	2	9	11
Stack 2	bridge_x_2a	FC1	1	10	14
		FC2	2	10	14
	bridge_x_2B	FC1	1	11	15
		FC2	2	11	15
Stack 3	bridge_x_3a	FC1	1	12*	16
		FC2	2	12*	16
	bridge_x_3B	FC1	1	13*	17
		FC2	2	13*	17
Stack y	bridge_x_ya	FC1	1	14*	20
		FC2	2	14*	20
	bridge_x_yb	FC1	1	15*	21
		FC2	2	15*	21

* Ports 12 through 15 are reserved for the second MetroCluster or DR group on the Brocade 7840 switch.

Additional bridges can be cabled to ports 16, 17, 20 and 21 in G620, G630, G620-1 and G630-1 switches.

Configurations using FibreBridge 7500N or 7600N using both FC ports (FC1 and FC2)

MetroCluster 2 or DR Group 2							
Component	**Port**	**Brocade switch model**					
		Connects to FC_switch…	**6510, DCX 8510-8**	**6520**	**7840, DCX 8510-8**	**G620, G620-1, G630, G630-1**	**G720**
controller_x_3	FC-VI port a	1	24	48	12	18	18
	FC-VI port b	2	24	48	12	18	18
	FC-VI port c	1	25	49	13	19	19
	FC-VI port d	2	25	49	13	19	19
	HBA port a	1	26	50	14	24	26
	HBA port b	2	26	50	14	24	26
	HBA port c	1	27	51	15	25	27
	HBA port d	2	27	51	15	25	27

controller_x_4		FC-VI port a	1	28	52	16	22	22
		FC-VI port b	2	28	52	16	22	22
		FC-VI port c	1	29	53	17	23	23
		FC-VI port d	2	29	53	17	23	23
		HBA port a	1	30	54	18	28	30
		HBA port b	2	30	54	18	28	30
		HBA port c	1	31	55	19	29	31
		HBA port d	2	31	55	19	29	31
Stack 1	bridge_x_51a	FC1	1	32	56	20	26	32
		FC2	2	32	56	20	26	32
	bridge_x_51b	FC1	1	33	57	21	27	33
		FC2	2	33	57	21	27	33
Stack 2	bridge_x_52a	FC1	1	34	58	22	30	34
		FC2	2	34	58	22	30	34
	bridge_x_52b	FC1	1	35	59	23	31	35
		FC2	2	35	59	23	31	35

Stack 3	bridge_x_53a	FC1	1	36	60	-	32	36
		FC2	2	36	60	-	32	36
	bridge_x_53b	FC1	1	37	61	-	33	37
		FC2	2	37	61	-	33	37
Stack y	bridge_x_5ya	FC1	1	38	62	-	34	38
		FC2	2	38	62	-	34	38
	bridge_x_5yb	FC1	1	39	63	-	35	39
		FC2	2	39	63	-	35	39
Additional bridges can be cabled to ports 36 to 39 in G620, G630, G620-1, and G630-1 switches.								

Brocade port usage for ISLs in a MetroCluster configuration running ONTAP 9.1 or later

The following table shows ISL port usage for the Brocade switches.

AFF A700 or FAS9000 systems support up to eight ISLs for improved performance. Eight ISLs are supported on the Brocade 6510 and G620 switches.

Switch model	ISL port	Switch port
Brocade 6520	ISL port 1	23
	ISL port 2	47
	ISL port 3	71
	ISL port 4	95
Brocade 6505	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23

Switch model	ISL port	Switch port
Brocade 6510 and Brocade DCX 8510-8	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47
Brocade 7810	ISL port 1	ge2 (10-Gbps)
	ISL port 2	ge3(10-Gbps)
	ISL port 3	ge4 (10-Gbps)
	ISL port 4	ge5 (10-Gbps)
	ISL port 5	ge6 (10-Gbps)
	ISL port 6	ge7 (10-Gbps)
Brocade 7840 **Note**: The Brocade 7840 switch supports either two 40 Gbps VE-ports or up to four 10 Gbps VE-ports per switch for the creation of FCIP ISLs.	ISL port 1	ge0 (40-Gbps) or ge2 (10-Gbps)
	ISL port 2	ge1 (40-Gbps) or ge3 (10-Gbps)
	ISL port 3	ge10 (10-Gbps)
	ISL port 4	ge11 (10-Gbps)
Brocade G610	ISL port 1	20
	ISL port 2	21
	ISL port 3	22
	ISL port 4	23

Switch model	ISL port	Switch port
Brocade G620, G620-1, G630, G630-1, G720	ISL port 1	40
	ISL port 2	41
	ISL port 3	42
	ISL port 4	43
	ISL port 5	44
	ISL port 6	45
	ISL port 7	46
	ISL port 8	47

Cisco port usage for controllers in a MetroCluster configuration running ONTAP 9.4 or later

The tables show the maximum supported configurations, with eight controller modules in two DR groups. For smaller configurations, ignore the rows for the additional controller modules.

Cisco 9396S			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	
	HBA port d	-	8
controller_x_3	FC-VI port a	49	
	FC-VI port b	-	49
	FC-VI port c	50	-
	FC-VI port d	-	50
	HBA port a	51	-
	HBA port b	-	51
	HBA port c	52	
	HBA port d	-	52

controller_x_4	FC-VI port a	53	-
	FC-VI port b	-	53
	FC-VI port c	54	-
	FC-VI port d	-	54
	HBA port a	55	-
	HBA port b	-	55
	HBA port c	56	-
	HBA port d	-	56

Cisco 9148S			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8
controller_x_3	FC-VI port a	25	
	FC-VI port b	-	25
	FC-VI port c	26	-
	FC-VI port d	-	26
	HBA port a	27	-
	HBA port b	-	27
	HBA port c	28	-
	HBA port d	-	28

controller_x_4	FC-VI port a	29	-
	FC-VI port b	-	29
	FC-VI port c	30	-
	FC-VI port d	-	30
	HBA port a	31	-
	HBA port b	-	31
	HBA port c	32	-
	HBA port d	-	32

Cisco 9132T			
MDS module 1			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_2	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8
		MDS module 2	
Component	Port	Switch 1	Switch 2
controller_x_3	FC-VI port a	1	-
	FC-VI port b	-	1
	FC-VI port c	2	-
	FC-VI port d	-	2
	HBA port a	3	-
	HBA port b	-	3
	HBA port c	4	-
	HBA port d	-	4

controller_x_4	FC-VI port a	5	-
	FC-VI port b	-	5
	FC-VI port c	6	-
	FC-VI port d	-	6
	HBA port a	7	-
	HBA port b	-	7
	HBA port c	8	-
	HBA port d	-	8

The following table shows systems with two FC-VI ports. AFF A700 and FAS9000 systems have four FC-VI ports (a, b, c, and d). If using an AFF A700 or FAS9000 system, the port assignments move along by one position. For example, FC-VI ports c and d go to switch port 2 and HBA ports a and b go to switch port 3.

Cisco 9250i **Note: The Cisco 9250i switch is not supported for eight-node MetroCluster configurations.**			
Component	**Port**	**Switch 1**	**Switch 2**
controller_x_1	FC-VI port a	1	-
	FC-VI port b	-	1
	HBA port a	2	-
	HBA port b	-	2
	HBA port c	3	-
	HBA port d	-	3

controller_x_2	FC-VI port a	4	-
	FC-VI port b	-	4
	HBA port a	5	-
	HBA port b	-	5
	HBA port c	6	-
	HBA port d	-	6
controller_x_3	FC-VI port a	7	-
	FC-VI port b	-	7
	HBA port a	8	-
	HBA port b	-	8
	HBA port c	9	-
	HBA port d	-	9
controller_x_4	FC-VI port a	10	-
	FC-VI port b	-	10
	HBA port a	11	-
	HBA port b	-	11
	HBA port c	13	-
	HBA port d	-	13

Cisco port usage for FC-to-SAS bridges in a MetroCluster configuration running ONTAP 9.1 or later

Cisco 9396S			
FibreBridge 7500 using two FC ports	**Port**	**Switch 1**	**Switch 2**

bridge_x_1a	FC1	9	-
	FC2	-	9
bridge_x_1b	FC1	10	-
	FC2	-	10
bridge_x_2a	FC1	11	-
	FC2	-	11
bridge_x_2b	FC1	12	-
	FC2	-	12
bridge_x_3a	FC1	13	-
	FC2	-	13
bridge_x_3b	FC1	14	-
	FC2	-	14
bridge_x_4a	FC1	15	-
	FC2	-	15
bridge_x_4b	FC1	16	-
	FC2	-	16

Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.

Cisco 9148S			
FibreBridge 7500 using two FC ports	**Port**	**Switch 1**	**Switch 2**
bridge_x_1a	FC1	9	-
	FC2	-	9

bridge_x_1b	FC1	10	-
	FC2	-	10
bridge_x_2a	FC1	11	-
	FC2	-	11
bridge_x_2b	FC1	12	-
	FC2	-	12
bridge_x_3a	FC1	13	-
	FC2	-	13
bridge_x_3b	FC1	14	-
	FC2	-	14
bridge_x_4a	FC1	15	-
	FC2	-	15
bridge_x_4b	FC1	16	-
	FC2	-	16

Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 33 through 40 following the same pattern.

Cisco 9132T			
FibreBridge 7500 using two FC ports	**Port**	**Switch**	**Switch 2**
bridge_x_1a	FC1	9	-
	FC2	-	9
bridge_x_1b	FC1	10	-
	FC2	-	10

bridge_x_2a	FC1	11	-
	FC2	-	11
bridge_x_2b	FC1	12	-
	FC2	-	12

Additional bridges for a second DR group or second MetroCluster configuration can be attached using the same port numbers on the second MDS module.

Cisco 9250i			
FibreBridge 7500 using two FC ports	**Port**	**Switch 1**	**Switch 2**
bridge_x_1a	FC1	14	-
	FC2	-	14
bridge_x_1b	FC1	15	-
	FC2	-	15
bridge_x_2a	FC1	17	-
	FC2	-	17
bridge_x_2b	FC1	18	-
	FC2	-	18
bridge_x_3a	FC1	19	-
	FC2	-	19
bridge_x_3b	FC1	21	-
	FC2	-	21
bridge_x_4a	FC1	22	-
	FC2	-	22

bridge_x_4b	FC1	23	-
	FC2	-	23

Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 25 through 48 following the same pattern.

The following tables show bridge port usage when using FibreBridge 6500 bridges or FibreBridge 7500 bridges using one FC port (FC1 or FC2) only. For FibreBridge 7500 bridges using one FC port, either FC1 or FC2 can be cabled to the port indicated as FC1. Additional bridges can be attached using ports 25-48.

FibreBridge 6500 bridges or FibreBridge 7500 bridges using one FC port			
FibreBridge 6500 bridge or FibreBridge 7500 using one FC port	**Port**	**Cisco 9396S**	
		Switch 1	**Switch 2**
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-

bridge_x_8b	FC1	-	16

Additional bridges can be attached using ports 17 through 40 and 57 through 88 following the same pattern.

FibreBridge 6500 bridges or FibreBridge 7500 bridges using one FC port			
Bridge	**Port**	**Cisco 9148S**	
		Switch 1	**Switch 2**
bridge_x_1a	FC1	9	-
bridge_x_1b	FC1	-	9
bridge_x_2a	FC1	10	-
bridge_x_2b	FC1	-	10
bridge_x_3a	FC1	11	-
bridge_x_3b	FC1	-	11
bridge_x_4a	FC1	12	-
bridge_x_4b	FC1	-	12
bridge_x_5a	FC1	13	-
bridge_x_5b	FC1	-	13
bridge_x_6a	FC1	14	-
bridge_x_6b	FC1	-	14
bridge_x_7a	FC1	15	-
bridge_x_7b	FC1	-	15
bridge_x_8a	FC1	16	-
bridge_x_8b	FC1	-	16

Additional bridges for a second DR group or second MetroCluster configuration can be attached using ports 25 through 48 following the same pattern.

Cisco 9250i

FibreBridge 6500 bridge or FibreBridge 7500 using one FC port	Port	Switch 1	Switch 2
bridge_x_1a	FC1	14	-
bridge_x_1b	FC1	-	14
bridge_x_2a	FC1	15	-
bridge_x_2b	FC1	-	15
bridge_x_3a	FC1	17	-
bridge_x_3b	FC1	-	17
bridge_x_4a	FC1	18	-
bridge_x_4b	FC1	-	18
bridge_x_5a	FC1	19	-
bridge_x_5b	FC1	-	19
bridge_x_6a	FC1	21	-
bridge_x_6b	FC1	-	21
bridge_x_7a	FC1	22	-
bridge_x_7b	FC1	-	22
bridge_x_8a	FC1	23	-
bridge_x_8b	FC1	-	23

Additional bridges can be attached using ports 25 through 48 following the same pattern.

Cisco port usage for ISLs in an eight-node configuration in a MetroCluster configuration running ONTAP 9.1 or later

The following table shows ISL port usage. ISL port usage is the same on all switches in the configuration.

Switch model	ISL port	Switch port

Cisco 9396S	ISL 1	44
	ISL 2	48
	ISL 3	92
	ISL 4	96
Cisco 9250i with 24 port license	ISL 1	12
	ISL 2	16
	ISL 3	20
	ISL 4	24
Cisco 9148S	ISL 1	20
	ISL 2	24
	ISL 3	44
	ISL 4	48
Cisco 9132T	ISL 1	MDS module 1 port 13
	ISL 2	MDS module 1 port 14
	ISL 3	MDS module 1 port 15
	ISL 4	MDS module 1 port 16

Using the Interoperability Matrix Tool to find MetroCluster information

When setting up the MetroCluster configuration, you can use the Interoperability Tool to ensure you are using supported software and hardware versions.

NetApp Interoperability Matrix Tool

After opening the Interoperability Matrix, 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.

Where to find additional information

You can learn more about configuring, operating, and monitoring a MetroCluster configuration in NetApp's extensive documentation library.

Guide	Content
MetroCluster documentation	• All MetroCluster guides
NetApp MetroCluster Solution Architecture and Design	• A technical overview of the MetroCluster configuration and operation. • Best practices for MetroCluster 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
Stretch MetroCluster installation and configuration	• Stretch MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • Configuring the MetroCluster in ONTAP
MetroCluster IP installation and configuration	• MetroCluster IP architecture • Cabling the MetroCluster IP configuration • Configuring the MetroCluster in ONTAP
NetApp Documentation: Product Guides and Resources	• Monitoring the MetroCluster configuration and performance
MetroCluster Tiebreaker Software Installation and Configuration Guide	• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software
Copy-based transition	• Transitioning data from 7-Mode storage systems to clustered storage systems

MetroCluster® Transition Guide

This content provides procedures for transitioning from a MetroCluster FC to a MetroCluster IP configuration.

Supported platforms for nondisruptive transition

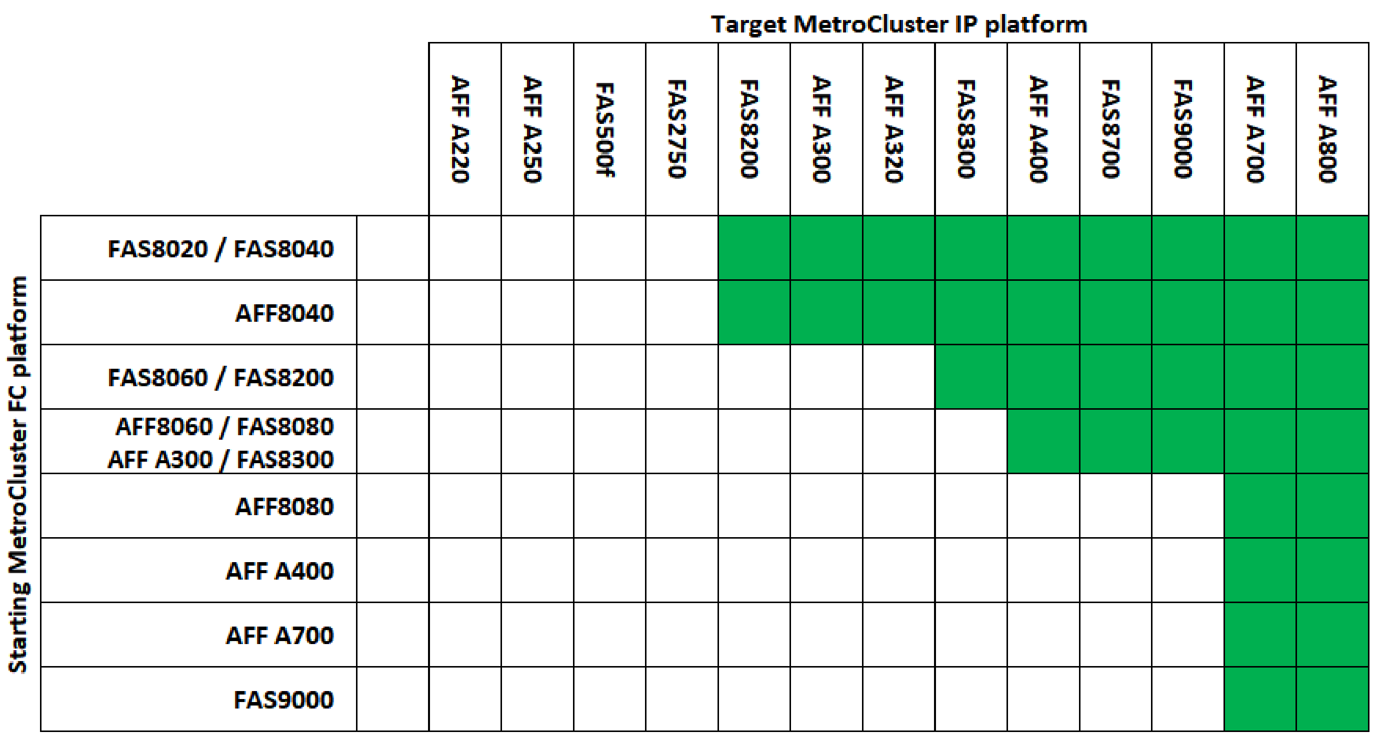
When transitioning to a MetroCluster IP configuration, you must have a combination of supported platform models.

The following table shows the supported platform combinations. You can transition from platforms in the left-hand column to platforms listed as supported in the columns to the right, as indicated by the green table cells.

- A green cell shows that the combination is supported.
- A white (blank) cell indicates that the combination is unsupported.

For example, transitioning from a MetroCluster FC configuration consisting of AFF8060 controller modules to an IP configuration consisting of AFF A400 controller modules is supported.

> Transitioning to a Cisco 9336C-FX2 shared switch configuration is not supported.



Transitioning nondisruptively from a MetroCluster FC to a MetroCluster IP configuration (ONTAP 9.8 and later)

Starting with ONTAP 9.8, nondisruptive transition of workloads and data from an existing four-node MetroCluster FC configuration to a new MetroCluster IP configuration is supported.

- This procedure is supported on systems running ONTAP 9.8 and later.
- This procedure is nondisruptive.

  The MetroCluster configuration can continue to serve data during the operation.

- This procedure applies only to four-node MetroCluster FC configurations.

  If you have a two-node MetroCluster FC configuration, see Choosing your transition procedure.

- You must meet all requirements and follow all steps in the procedure.

Preparing for transition from a MetroCluster FC to a MetroCluster IP configuration

As you prepare for the MetroCluster transition, you should understand the requirements and the steps involved.

Requirements for nondisruptive FC-to-IP transition

Before starting the transition process, you must make sure the configuration meets the requirements.

- It must be a four-node configuration and all nodes must be running ONTAP 9.8 or later.
- The existing and new platforms must be a supported combination for transition.

  Supported platforms for nondisruptive transition

- It must support a switched cluster configuration.

  NetApp Hardware Universe

- It must meet all requirements and cabling as described in the *MetroCluster Installation and Configuration Guides*.

  Fabric-attached MetroCluster installation and configuration

  Stretch MetroCluster installation and configuration

How transition impacts the MetroCluster hardware components

After completing the transition procedure, key components of the existing MetroCluster configuration have been replaced or reconfigured.

- **Controller modules**

  The existing controller modules are replaced by new controller modules. The existing controller modules are decommissioned at the end of the transition procedures.

- **Storage shelves**

  Data is moved from the old shelves to the new shelves. The old shelves are decommissioned at the end of the transition procedures.

- **MetroCluster (back-end) and cluster switches**

  The back-end switch functionality is replaced by the IP switch fabric. If the MetroCluster FC configuration included FC switches and FC-to-SAS bridges, they are decommissioned at the end of this procedure.

  If the MetroCluster FC configuration used cluster switches for the cluster interconnect, in some cases they can be reused to provide the back-end IP switch fabric. Reused cluster switches must be reconfigured with platform and switch-specific RCFs. procedures.

  If the MetroCluster FC configuration did not use cluster switches, new IP switches are added to provide the backend switch fabric.

  Considerations for IP switches

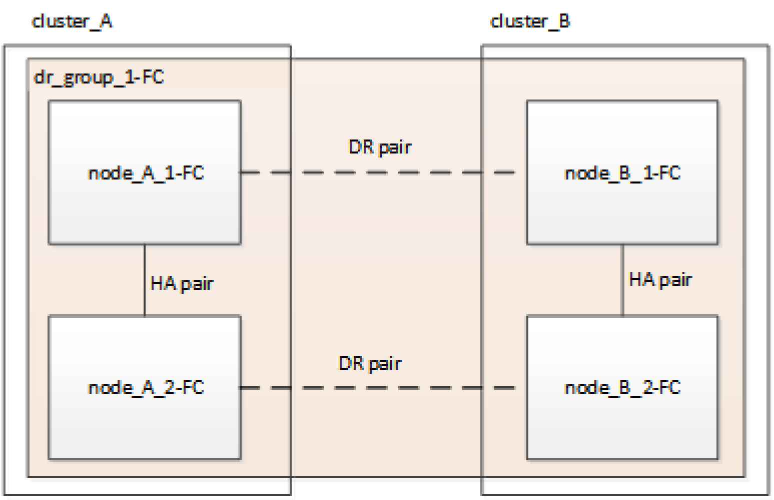
- **Cluster peering network**

  The existing customer-provided cluster peering network can be used for the new MetroCluster IP configuration. Cluster peering is configured on the MetroCluster IP nodes as part of the transition procedure.

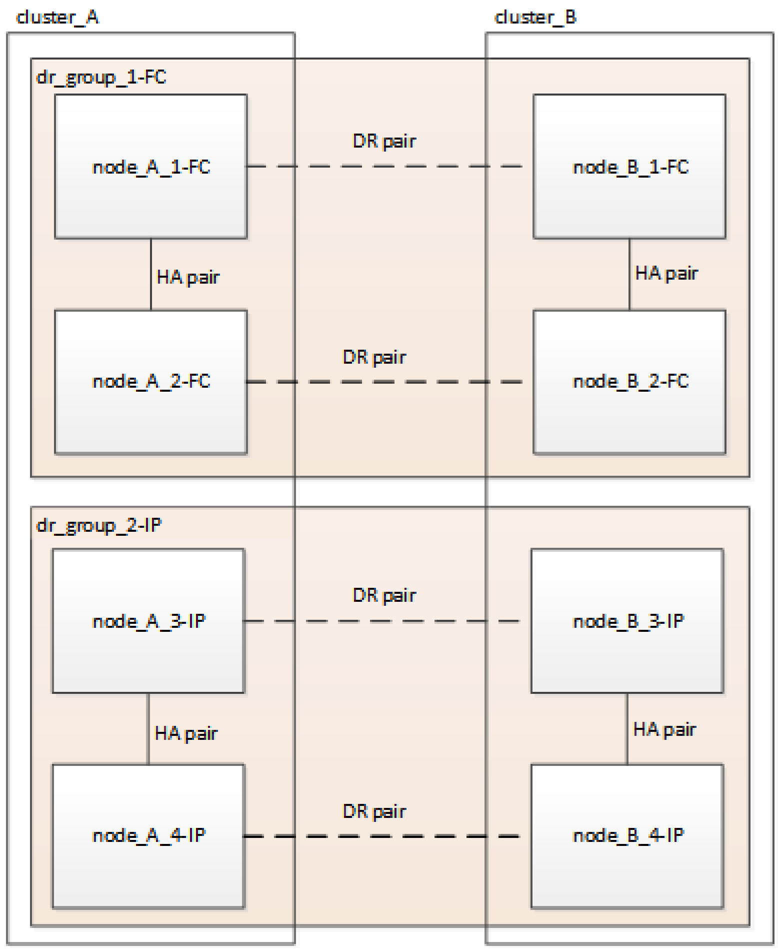
Workflow for nondisruptive MetroCluster transition

You must follow the specific workflow to ensure a successful nondisruptive transition.

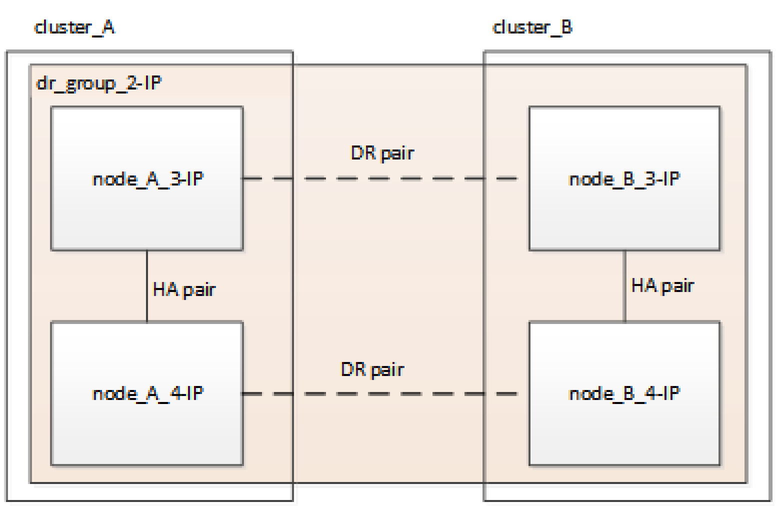
The transition process begins with a healthy four-node MetroCluster FC configuration.



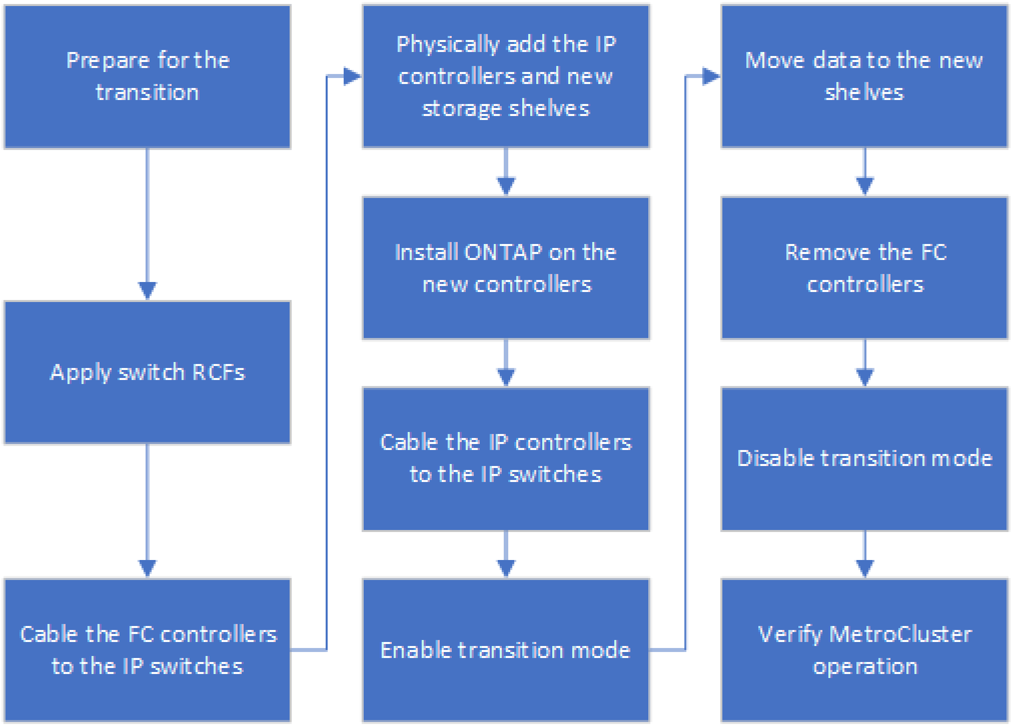
The new MetroCluster IP nodes are added as a second DR group.



Data is transferred from the old DR group to the new DR group, and then the old nodes and their storage are removed from the configuration and decommissioned. The process ends with a four-node MetroCluster IP configuration.



You will use the following workflow to transition the MetroCluster configuration.



Considerations for IP switches

You must ensure the IP switches are supported. If the existing switch model is supported by both the original MetroCluster FC configuration and the new MetroCluster IP configuration, you can reuse the existing switches.

Supported switches

You must use NetApp-provided switches.

- The use of MetroCluster-compliant switches (switches that are not validated and provided by NetApp) is not supported for transition.
- The IP switches must be supported as a cluster switch by both the MetroCluster FC configuration and the MetroCluster IP configuration.
- The IP switches can be reused in the new MetroCluster IP configuration if the MetroCluster FC is a switched cluster and the IP cluster switches are supported by the MetroCluster IP configuration.
- New IP switches are usually used in the following cases:
  - The MetroCluster FC is a switchless cluster, so new switches are required.
  - The MetroCluster FC is a switched cluster but the existing IP switches are not supported in the MetroCluster IP configuration.
  - You want to use different switches for the MetroCluster IP configuration.

See the *NetApp Hardware Universe* for information on platform model and switch support.

NetApp Hardware Universe

Switchover, healing, and switchback operations during nondisruptive transition

Depending on the stage of the transition process, the MetroCluster switchover, healing, and switchback operations use either the MetroCluster FC or MetroCluster IP workflow.

The following table shows what workflows are used at different stages of the transition process. In some stages, switchover and switchback are not supported.

- In the MetroCluster FC workflow, the switchover, healing and switchback steps are those used by a MetroCluster FC configuration.
- In the MetroCluster IP workflow, the switchover, healing and switchback steps are those used by a MetroCluster IP configuration.
- In the unified workflow, when both the FC and IP nodes are configured, the steps depend on whether NSO or USO is performed. The details are shown in the table.

For information on the MetroCluster FC and IP workflows for switchover, healing, and switchback, see Understanding MetroCluster data protection and disaster recovery.

> Automatic unplanned switchover is not available during the transition process.

Stage of transition	Negotiated switchover uses… this workflow	Unplanned switchover uses this workflow…
Before the MetroCluster IP nodes have joined the cluster.	MetroCluster FC	MetroCluster FC
After the MetroCluster IP nodes have joined the cluster, before the metrocluster configure command is performed.	Not supported	MetroCluster FC
After the metrocluster configure command has been issued. Volume move can be in progress.	Unified:All remote site nodes remain up and healing is done automatically	Unified: • Mirrored aggregates owned by the MetroCluster FC node are mirrored if storage is accessible, all others are degraded after switchover • All remote site nodes are able to boot up. • Heal aggregate and heal root commands must be run manually.
The MetroCluster FC nodes have been unconfigured.	Not supported	MetroCluster IP
The cluster unjoin command has been performed on the MetroCluster FC nodes.	MetroCluster IP	MetroCluster IP

Alert messages and tool support during transition

You may notice alert messages during transition. These alerts can be safely ignored. Also, some tools are not available during transition.

- ARS may alert during transition.

  These alerts can be ignored and should disappear once the transition has finished.

- OnCommand Unified Manager may alert during transition.

  These alerts can be ignored and should disappear once the transition has finished.

- Config Advisor is not supported during transition.
- System Manager is not supported during transition.

Example naming in this procedure

This procedure uses example names throughout to identify the DR groups, nodes, and switches involved.

DR groups	cluster_A at site_A	cluster_B at site_B
dr_group_1-FC	• node_A_1-FC • node_A_2-FC	• node_B_1-FC • node_B_2-FC
dr_group_2-IP	• node_A_3-IP • node_A_4-IP	• node_B_3-IP • node_B_4-IP
Switches	Initial switches (if fabric-attached configuration:) • switch_A_1-FC • switch_A_2-FC MetroCluster IP switches: • switch_A_1-IP • switch_A_2-IP	Initial switches (if fabric-attached configuration): • switch_B_1-FC • switch_B_2-FC MetroCluster IP switches: • switch_B_1-IP • switch_B_2-IP

Transitioning from MetroCluster FC to MetroCluster IP configurations

After reviewing all requirements and preparing for the transition, you perform the transition procedure. You must perform each task in order, completing all steps in each task before moving to the next. You should not connect the new controllers or storage shelves to the existing configuration until directed.

Verifying the health of the MetroCluster configuration

You must verify the health and connectivity of the MetroCluster configuration prior to performing the transition

1. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:`node run -node node-name sysconfig -a`
   b. Check for any health alerts on both clusters: `system health alert show`
   c. Confirm the MetroCluster configuration and that the operational mode is normal: `metrocluster show`
   d. Perform a MetroCluster check: `metrocluster check run`
   e. Display the results of the MetroCluster check: `metrocluster check show`
   f. Check for any health alerts on the switches (if present): `storage switch show`
   g. Run Config Advisor.

      NetApp Downloads: Config Advisor
   h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
2. Verify that the cluster is healthy: `cluster show`

```
cluster_A::> cluster show
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1_FC    true    true          false
node_A_2_FC    true    true          false

cluster_A::>
```

3. Verify that all cluster ports are up: `network port show -ipspace cluster`

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1_FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                      Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verify that all cluster LIFs are up and operational: `network interface show -vserver cluster`

   Each cluster LIF should display "true" for "Is Home" and "up/up" for "Status Admin/Oper".

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A-1_FC_clus1
                       up/up      169.254.209.69/16  node_A-1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Verify that auto-revert is enabled on all cluster LIFs: `network interface show -vserver Cluster -fields auto-revert`

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1_FC_clus1
                        true
           node_A_1_FC_clus2
                        true
           node_A_2_FC_clus1
                        true
           node_A_2_FC_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Removing the existing configuration from the Tiebreaker or other monitoring software

If the existing configuration is monitored with the MetroCluster Tiebreaker configuration or other third-party applications (for example, ClusterLion) that can initiate a switchover, you must remove the MetroCluster configuration from the Tiebreaker or other software prior to transition.

1. Remove the existing MetroCluster configuration from the Tiebreaker software.

   Removing MetroCluster configurations

2. Remove the existing MetroCluster configuration from any third-party application that can initiate switchover.

   Refer to the documentation for the application.

Generating and applying RCFs to the new IP switches

If you are using new IP switches for the MetroCluster IP configuration, you must configure the switches with a custom RCF file.

This task is required if you are using new switches.

If you are using existing switches, proceed to Moving the local cluster connections.

1. Install and rack the new IP switches.
2. Prepare the IP switches for the application of the new RCF files.

   Follow the steps in the section for your switch vendor from the MetroCluster IP Installation and

Configuration Guide

  ◦ Resetting the Broadcom IP switch to factory defaults
  ◦ Resetting the Cisco IP switch to factory defaults

3. Update the firmware on the switch to a supported version, if necessary.
4. Use the RCF generator tool to create the RCF file depending on your switch vendor and the platform models, and then update the switches with the file.

   Follow the steps in the section for your switch vendor from the *MetroCluster IP Installation and Configuration guide*.

   MetroCluster IP installation and configuration

  ◦ Downloading and installing the Broadcom IP RCF files
  ◦ Downloading and installing the Cisco IP RCF files

Moving the local cluster connections

You must move the MetroCluster FC configuration’s cluster interfaces to the IP switches.

Moving the cluster connections on the MetroCluster FC nodes

You must move the cluster connections on the MetroCluster FC nodes to the IP switches. The steps depend on whether you are using the existing IP switches or you are using new IP switches.

You must perform this task on both MetroCluster sites.

The following task assumes a controller module using two ports for the cluster connections. Some controller module models use four or more ports for the cluster connection. In that case, for the purposes of this example, the ports are divided into two groups, alternating ports between the two groups

The following table shows the example ports used in this task.

Number of cluster connections on the controller module	Group A ports	Group B ports
Two	e0a	e0b
Four	e0a, e0c	e0b, e0d

- Group A ports connect to local switch switch_x_1-IP.
- Group B ports connect to local switch switch_x_2-IP.

The following table shows which switch ports the FC nodes connect to. For the Broadcom BES-53248 switch, the port usage depends on the model of the MetroCluster IP nodes.

Switch model	MetroCluster IP node model	Switch port(s)	Connects to
Cisco 3132Q-V or 3232C	Any	5	node_x_1-FC
		6	node_x_2-FC
Broadcom BES-53248	FAS2750/A220	1, 2, 3	node_x_1-FC
	FAS8200 / A300	1, 2, 3, 7, 8, 9	node_x_1-FC
	FAS2750/A220	4, 5, 6	node_x_2-FC
	FAS8200 / A300	4, 5, 6, 10, 11, 12	node_x_2-FC

Moving the local cluster connections when using new IP switches

If you are using new IP switches, you must physically move the existing MetroCluster FC nodes' cluster connections to the new switches.

1. Move the MetroCluster FC node group A cluster connections to the new IP switches.

   Use the ports described in Moving the cluster connections on the MetroCluster FC nodes.

   a. Disconnect all the group A ports from the switch, or, if the MetroCluster FC configuration was a switchless cluster, disconnect them from the partner node.

   b. Disconnect the group A ports from node_A_1-FC and node_A_2-FC.

   c. Connect the group A ports of node_A_1-FC to the switch ports for the FC node on switch_A_1-IP

   d. Connect the group A ports of node_A_2-FC to the switch ports for the FC node on switch_A_1-IP

2. Verify that all cluster ports are up: `network port show -ipspace Cluster`

```
cluster_A::*> network port show -ipspace Cluster

Node: node_A_1-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-FC

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::*>
```

3. Verify that all interfaces display true in the Is Home column: `network interface show -vserver cluster`

   This might take several minutes to complete.

```
cluster_A::*> network interface show -vserver cluster

            Logical       Status     Network            Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1-FC_clus2
                       up/up      169.254.49.125/16  node_A_1-FC   e0b
true
            node_A_2-FC_clus1
                       up/up      169.254.47.194/16  node_A_2-FC   e0a
true
            node_A_2-FC_clus2
                       up/up      169.254.19.183/16  node_A_2-FC   e0b
true

4 entries were displayed.

cluster_A::*>
```

4. Perform the above steps on both nodes (node_A_1-FC and node_A_2-FC) to move the group B ports of the cluster interfaces.
5. Repeat the above steps on the partner cluster "cluster_B".

Moving the local cluster connections when reusing existing IP switches

If you are reusing existing IP switches, you must update firmware, reconfigure the switches with the correct Reference Configure Files (RCFs) and move the connections to the correct ports one switch at a time.

This task is required only if the FC nodes are connected to existing IP switches and you are reusing the switches.

1. Disconnect the local cluster connections that connect to switch_A_1_IP
   a. Disconnect the group A ports from the existing IP switch.
   b. Disconnect the ISL ports on switch_A_1_IP.

      You can see the Installation and Setup instructions for the platform to see the cluster port usage.

      AFF A320 systems: Installation and setup

AFF A220/FAS2700 Systems Installation and Setup Instructions

AFF A800 Systems Installation and Setup Instructions

AFF A300 Systems Installation and Setup Instructions

FAS8200 Systems Installation and Setup Instructions

2. Reconfigure switch_A_1_IP using RCF files generated for your platform combination and transition.

   Follow the steps in the section for your switch vendor from the *MetroCluster IP Installation and Configuration guide*, as given in the links below.

   MetroCluster IP installation and configuration

   a. If required, download and install the new switch firmware.

      You should use the latest firmware that the MetroCluster IP nodes support.

      - Downloading and installing the Broadcom switch EFOS software
      - Downloading and installing the Cisco switch NX-OS software

   b. Prepare the IP switches for the application of the new RCF files.

      - Resetting the Broadcom IP switch to factory defaults **
      - Resetting the Cisco IP switch to factory defaults

   c. Download and install the IP RCF file depending on your switch vendor.

      - Downloading and installing the Broadcom IP RCF files
      - Downloading and installing the Cisco IP RCF files

3. Reconnect the group A ports to switch_A_1_IP.

   Use the ports described in Moving the cluster connections on the MetroCluster FC nodes.

4. Verify that all cluster ports are up: `network port show -ipspace cluster`

```
Cluster-A::*> network port show -ipspace cluster

Node: node_A_1_FC

                                                     Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2_FC

                                                     Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

5. Verify that all interfaces are on their home port: `network interface show -vserver Cluster`

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1_FC_clus1
                       up/up      169.254.209.69/16  node_A_1_FC   e0a
true
            node_A_1_FC_clus2
                       up/up      169.254.49.125/16  node_A_1_FC   e0b
true
            node_A_2_FC_clus1
                       up/up      169.254.47.194/16  node_A_2_FC   e0a
true
            node_A_2_FC_clus2
                       up/up      169.254.19.183/16  node_A_2_FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

6. Repeat all the previous steps on switch_A_2_IP.
7. Reconnect the local cluster ISL ports.
8. Repeat the above steps at site_B for switch B_1_IP and switch B_2_IP.
9. Connect the remote ISLs between the sites.

Verifying that the cluster connections are moved and the cluster is healthy

To ensure that there is proper connectivity and that the configuration is ready to proceed with the transition process, you must verify that the cluster connections are moved correctly, the cluster switches are recognized and the cluster is healthy.

1. Verify that all cluster ports are up and running: `network port show -ipspace Cluster`

```
Cluster-A::*> network port show -ipspace Cluster

Node: Node-A-1-FC

                                                Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: Node-A-2-FC

                                                Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

Cluster-A::*>
```

2. Verify that all interfaces are on their home port: `network interface show -vserver Cluster`

   This might take several minutes to complete.

   The following example shows that all interfaces show true in the Is Home column.

```
Cluster-A::*> network interface show -vserver Cluster

            Logical      Status     Network          Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            Node-A-1_FC_clus1
                       up/up      169.254.209.69/16  Node-A-1_FC   e0a
true
            Node-A-1-FC_clus2
                       up/up      169.254.49.125/16  Node-A-1-FC   e0b
true
            Node-A-2-FC_clus1
                       up/up      169.254.47.194/16  Node-A-2-FC   e0a
true
            Node-A-2-FC_clus2
                       up/up      169.254.19.183/16  Node-A-2-FC   e0b
true

4 entries were displayed.

Cluster-A::*>
```

3. Verify that both the local IP switches are discovered by the nodes: `network device-discovery show -protocol cdp`

```
Cluster-A::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
Node-A-1-FC
           /cdp
            e0a    Switch-A-3-IP             1/5/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/5/1             N3K-
C3232C
Node-A-2-FC
           /cdp
            e0a    Switch-A-3-IP             1/6/1             N3K-
C3232C
            e0b    Switch-A-4-IP             0/6/1             N3K-
C3232C

4 entries were displayed.

Cluster-A::*>
```

4. On the IP switch, verify that the MetroCluster IP nodes have been discovered by both local IP switches: `show cdp neighbors`

   You must perform this step on each switch.

   This example shows how to verify the nodes are discovered on Switch-A-3-IP.

```
(Switch-A-3-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H          FAS8200       e0a
Node-A-2-FC         Eth1/6/1       133    H          FAS8200       e0a
Switch-A-4-IP(FDO220329A4)
                    Eth1/7         175    R S I s    N3K-C3232C    Eth1/7
Switch-A-4-IP(FDO220329A4)
                    Eth1/8         175    R S I s    N3K-C3232C    Eth1/8
Switch-B-3-IP(FDO220329B3)
                    Eth1/20        173    R S I s    N3K-C3232C
Eth1/20
Switch-B-3-IP(FDO220329B3)
                    Eth1/21        173    R S I s    N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-3-IP)#
```

This example shows how to verify that the nodes are discovered on Switch-A-4-IP.

```
(Switch-A-4-IP)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
Node-A-1-FC         Eth1/5/1       133    H          FAS8200       e0b
Node-A-2-FC         Eth1/6/1       133    H          FAS8200       e0b
Switch-A-3-IP(FDO220329A3)
                    Eth1/7         175    R S I s    N3K-C3232C    Eth1/7
Switch-A-3-IP(FDO220329A3)
                    Eth1/8         175    R S I s    N3K-C3232C    Eth1/8
Switch-B-4-IP(FDO220329B4)
                    Eth1/20        169    R S I s    N3K-C3232C
Eth1/20
Switch-B-4-IP(FDO220329B4)
                    Eth1/21        169    R S I s    N3K-C3232C
Eth1/21

Total entries displayed: 4

(Switch-A-4-IP)#
```

Preparing the MetroCluster IP controllers

You must prepare the four new MetroCluster IP nodes and install the correct ONTAP version.

This task must be performed on each of the new nodes:

- node_A_1-IP
- node_A_2-IP
- node_B_1-IP
- node_B_2-IP

In these steps, you clear the configuration on the nodes and clear the mailbox region on new drives.

1. Rack the new controllers for the MetroCluster IP configuration.

   The MetroCluster FC nodes (node_A_x-FC and node_B_x-FC) remain cabled at this time.

2. Cable the MetroCluster IP nodes to the IP switches as shown in the Cabling the IP switches.
3. Configure the MetroCluster IP nodes using the following sections:

a. Gathering required information
b. Clearing the configuration on a controller module
c. Verifying the ha-config state of components
d. Manually assigning drives for pool 0 (ONTAP 9.4 and later)

4. From Maintenance mode, issue the halt command to exit Maintenance mode, and then issue the boot_ontap command to boot the system and get to cluster setup.

   Do not complete the cluster wizard or node wizard at this time.

5. Repeat these steps on the other MetroCluster IP nodes.

Configure the MetroCluster for transition

To prepare the configuration for transition you add the new nodes to the existing MetroCluster configuration and then move data to the new nodes.

Sending a custom AutoSupport message prior to maintenance

Before performing the maintenance, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

This task must be performed on each MetroCluster site.

1. To prevent automatic support case generation, send an Autosupport message to indicate maintenance is underway.

   a. Issue the following command: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      maintenance-window-in-hours specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Repeat the command on the partner cluster.

Enabling transition mode and disabling cluster HA

You must enable the MetroCluster transition mode to allow the old and new nodes to operate together in the MetroCluster configuration, and disable cluster HA.

1. Enable transition:

   a. Change to the advanced privilege level: `set -privilege advanced`

   b. Enable transition mode: `metrocluster transition enable -transition-mode non-disruptive`

      Run this command on one cluster only.

```
cluster_A::*> metrocluster transition enable -transition-mode non-
disruptive

Warning: This command enables the start of a "non-disruptive"
MetroCluster
         FC-to-IP transition. It allows the addition of hardware for
another DR
         group that uses IP fabrics, and the removal of a DR group
that uses FC
         fabrics. Clients will continue to access their data during a
         non-disruptive transition.

         Automatic unplanned switchover will also be disabled by this
command.
Do you want to continue? {y|n}: y

cluster_A::*>
```

c. Return to the admin privilege level: `set -privilege admin`

2. Verify that transition is enabled on both the clusters.

```
cluster_A::> metrocluster transition show-mode
Transition Mode

non-disruptive

cluster_A::*>


cluster_B::*> metrocluster transition show-mode
Transition Mode

non-disruptive

Cluster_B::>
```

3. Disable cluster HA.

> You must run this command on both clusters.

```
cluster_A::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_A::*>


cluster_B::*> cluster ha modify -configured false

Warning: This operation will unconfigure cluster HA. Cluster HA must be
configured on a two-node cluster to ensure data access availability in
the event of storage failover.
Do you want to continue? {y|n}: y
Notice: HA is disabled.

cluster_B::*>
```

4. Verify that cluster HA is disabled.

   You must run this command on both clusters.

```
cluster_A::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_A::>

cluster_B::> cluster ha show

High Availability Configured: false
Warning: Cluster HA has not been configured. Cluster HA must be
configured
on a two-node cluster to ensure data access availability in the
event of storage failover. Use the "cluster ha modify -configured
true" command to configure cluster HA.

cluster_B::>
```

Joining the MetroCluster IP nodes to the clusters

You must add the four new MetroCluster IP nodes to the existing MetroCluster configuration.

You must perform this task on both clusters.

1. Add the MetroCluster IP nodes to the existing MetroCluster configuration.
   a. Join the first MetroCluster IP node (node_A_1-IP) to the existing MetroCluster FC configuration.

```
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.

This system will send event messages and periodic 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}: yes

Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:

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


Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e0c     9000    169.254.148.217 255.255.0.0
e0d     9000    169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

  b. Join the second MetroCluster IP node (node_A_2-IP) to the existing MetroCluster FC configuration.

2. Repeat these steps to join node_B_1-IP and node_B_2-IP to cluster_B.

You must create cluster peering LIFs, create the MetroCluster interfaces on the new MetroCluster IP nodes.

The home port used in the examples are platform-specific. You should use the appropriate home port specific to MetroCluster IP node platform.

1. On the new MetroCluster IP nodes, configure the intercluster LIFs.
2. On each site, verify that cluster peering is configured: `cluster peer show`

   The following example shows the cluster peering configuration on cluster_A:

```
cluster_A:> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B                  1-80-000011           Available      ok
```

   The following example shows the cluster peering configuration on cluster_B:

```
cluster_B:> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A 1-80-000011 Available ok
```

3. Configure the DR group for the MetroCluster IP nodes: `metrocluster configuration-settings dr-group create -partner-cluster`

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_3-IP -remote-node node_B_3-IP
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Verify that the DR group is created. `metrocluster configuration-settings dr-group show`

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                    Node               DR Partner
Node
----------- -------------------------- ------------------
------------------
2           cluster_A
                                       node_A_3-IP        node_B_3-IP
                                       node_A_4-IP        node_B_4-IP
            cluster_B
                                       node_B_3-IP        node_A_3-IP
                                       node_B_4-IP        node_A_4-IP

4 entries were displayed.

cluster_A::>
```

You will notice that the DR group for the old MetroCluster FC nodes (DR Group 1) is not listed when you run the `metrocluster configuration-settings dr-group show` command.

You can use `metrocluster node show` command on both sites to list all nodes.

```
cluster_A::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
      cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
2     cluster_A
              node_A_1-IP      ready to configure
                                                -         -
              node_A_2-IP      ready to configure
                                                -         -

cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1-FC         configured     enabled   normal
              node_B_2-FC         configured     enabled   normal
      cluster_A
              node_A_1-FC         configured     enabled   normal
              node_A_2-FC         configured     enabled   normal
2     cluster_B
              node_B_1-IP      ready to configure
                                                -         -
              node_B_2-IP      ready to configure
                                                -         -
```

5. Configure the MetroCluster IP interfaces for the newly joined MetroCluster IP nodes: `metrocluster configuration-settings interface create -cluster-name`

   See Configuring and connecting the MetroCluster IP interfaces for considerations when configuring the IP interfaces. NOTE: You can configure the MetroCluster IP interfaces from either cluster. Also, starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to xref:./transition/../install-ip/concept_considerations_layer_3.html.

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_3-IP -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_4-IP -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_3-IP -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_4-IP -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Verify the MetroCluster IP interfaces are created: `metrocluster configuration-settings interface show`

```
cluster_A::>metrocluster configuration-settings interface show

DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
2     cluster_A
             node_A_3-IP
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-IP
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_3-IP
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Connect the MetroCluster IP interfaces: `metrocluster configuration-settings connection connect`

This command might take several minutes to complete.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Verify the connections are properly established: `metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_A
              node_A_3-IP**
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_4-IP
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
```

```
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_4-IP
                 Home Port: e1a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e1a
                      172.17.26.13    172.17.26.11    DR Partner
completed
                 Home Port: e1a
                      172.17.26.13    172.17.26.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.12    HA Partner
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.11    DR Partner
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_3-IP
                 Home Port: e1a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e1a
                      172.17.26.12    172.17.26.10    DR Partner
completed
                 Home Port: e1a
                      172.17.26.12    172.17.26.11    DR Auxiliary
```

```
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.10    DR Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.11    DR Auxiliary
completed
24 entries were displayed.

cluster_A::>
```

9. Verify disk autoassignment and partitioning: `disk show -pool Pool1`

```
cluster_A::> disk show -pool Pool1
                     Usable            Disk     Container   Container
Disk                   Size Shelf Bay Type     Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                    -    10   4 SAS     remote      -
node_B_2
1.10.13                   -    10  13 SAS     remote      -
node_B_2
1.10.14                   -    10  14 SAS     remote      -
node_B_1
1.10.15                   -    10  15 SAS     remote      -
node_B_1
1.10.16                   -    10  16 SAS     remote      -
node_B_1
1.10.18                   -    10  18 SAS     remote      -
node_B_2
...
2.20.0              546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3              546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5              546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6              546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7              546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10             546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.

cluster_A::>
```

10. Mirror the root aggregates: `storage aggregate mirror -aggregate aggr0_node_A_3-IP`

> You must complete this step on each MetroCluster IP node.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_3-IP

Info: Disks would be added to aggregate "aggr0_node_A_3-IP"on node
"node_A_3-IP"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Verify that the root aggregates are mirrored: `storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-FC
           349.0GB   16.84GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr0_node_A_2-FC
           349.0GB   16.84GB   95% online       1 node_A_2-FC
```

```
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_4-IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-FC
raid_dp,

mirrored,
```

Finalizing the addition of the MetroCluster IP nodes

You must incorporate the new DR group into the MetroCluster configuration and create mirrored data aggregates on the new nodes.

1. Create mirrored data aggregates on each of the new MetroCluster nodes: `storage aggregate create -aggregate aggregate-name -node node-name -diskcount no-of-disks -mirror true`

   > You must create at least one mirrored data aggregate per site. It is recommended to have two mirrored data aggregates per site on MetroCluster IP nodes to host the MDV volumes, however a single aggregate per site is supported (but not recommended). It is support that one site of the MetroCluster has a single mirrored data aggregate and the other site has more than one mirrored data aggregate.

   The following example shows the creation of an aggregate on node_A_1-new.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-
new -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would
be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
-
          data       4.20.18                   SAS         546.9GB
547.1GB
          data       4.20.19                   SAS         546.9GB
547.1GB
          data       4.20.16                   SAS         546.9GB
547.1GB
```

```
      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

2. Configure the MetroCluster to implement the changes: `metrocluster configure`

```
cluster_A::*> metrocluster configure

[Job 439] Job succeeded: Configure is successful.

cluster_A::*>
```

3. Verify that the nodes are added to their DR group: `metrocluster node show`

```
cluster_A::*> metrocluster node show

DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node-A-1-FC        configured     enabled   normal
              node-A-2-FC        configured     enabled   normal
      Cluster-B
              node-B-1-FC        configured     enabled   normal
              node-B-2-FC        configured     enabled   normal
2     cluster_A
              node-A-3-IP        configured     enabled   normal
              node-A-4-IP        configured     enabled   normal
      Cluster-B
              node-B-3-IP        configured     enabled   normal
              node-B-4-IP        configured     enabled   normal
8 entries were displayed.

cluster_A::*>
```

4. Move the MDV_CRS volumes from the old nodes to the new nodes in advanced privilege.
   a. Display the volumes to identify the MDV volumes:

> ℹ If you have a single mirrored data aggregate per site then move both the MDV volumes to this single aggregate. If you have two or more mirrored data aggregates, then move each MDV volume to a different aggregate.

The following example shows the MDV volumes in the volume show output:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Set the advanced privilege level: `set -privilege advanced`

c. Move the MDV volumes, one at a time: `volume move start -volume mdv-volume -destination-aggregate aggr-on-new-node -vserver vserver-name`

   The following example shows the command and output for moving MDV_CRS_d6b0b313ff5611e9837100a098544e51_A to aggregate data_a3 on node_A_3.

```
cluster_A::> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Use the volume show command to check that the MDV volume has been successfully moved: `volume show mdv-name`

The following output shows that the MDV volume has been successfully moved.

```
cluster_A::> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
```

e. Return to admin mode: `set -privilege admin`

Moving the data to the new drive shelves

During the transition, you move data from the drive shelves in the MetroCluster FC configuration to the new MetroCluster IP configuration.

1. To resume automatic support case generation, send an Autosupport message to indicate that the maintenance is complete.
   a. Issue the following command: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Repeat the command on the partner cluster.
2. Move the data volumes to aggregates on the new controllers, one volume at a time.

   Use the following section of the *Controller Upgrade Express Guide*.

Creating an aggregate and moving volumes to the new nodes

3. Create SAN LIFs on the recently added nodes.

   Use the following section of the *Cluster Expansion Express Guide*.

   Updating LUN paths for the new nodes

4. Check if there are any node locked licenses on the FC nodes, if there are, they need to be added to the newly added nodes.

   Use the following section of the *Cluster Expansion Express Guide*.

   Adding node-locked licenses

5. Migrate the data LIFs.

   Use the following section of the *Controller Upgrade Express Guide* but do **not** perform the last two steps to migrate cluster management LIFs.

   Moving non-SAN data LIFs and cluster management LIFs to the new nodes

Removing the MetroCluster FC controllers

You must perform clean-up tasks and remove the old controller modules from the MetroCluster configuration.

1. To prevent automatic support case generation, send an Autosupport message to indicate maintenance is underway.

   a. Issue the following command: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      maintenance-window-in-hours specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Repeat the command on the partner cluster.

2. Identify the aggregates hosted on the MetroCluster FC configuration that need to be deleted.

   In this example the following data aggregates are hosted by the MetroCluster FC cluster_B and need to be deleted: aggr_data_a1 and aggr_data_a2.

   > You need to perform the steps to identify, offline and delete the data aggregates on both the clusters. The example is for one cluster only.

```
cluster_B::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
```

```
------------
aggr0_node_A_1-FC
           349.0GB   16.83GB   95% online       1 node_A_1-FC
raid_dp,

mirrored,

normal
aggr0_node_A_2-FC
           349.0GB   16.83GB   95% online       1 node_A_2-FC
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.63GB   95% online       1 node_A_3-IP
raid_dp,

mirrored,

normal
aggr0_node_A_3-IP
           467.6GB   22.62GB   95% online       1 node_A_4-IP
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.02TB    0% online       0 node_A_1-FC
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.02TB    0% online       0 node_A_2-FC
raid_dp,

mirrored,

normal
aggr_data_a3
            1.37TB    1.35TB    1% online       3 node_A_3-IP
raid_dp,
```

```
mirrored,

normal
aggr_data_a4
            1.25TB    1.24TB    1% online       2 node_A_4-IP
raid_dp,

mirrored,

normal
8 entries were displayed.

cluster_B::>
```

3. Check if the data aggregates on the FC nodes have any MDV_aud volumes, and delete them prior to deleting the aggregates.

   You must delete the MDV_aud volumes as they cannot be moved.

4. Take each of the aggregates offline, and then delete them:

   a. Take the aggregate offline: `storage aggregate offline -aggregate aggregate-name`

      The following example shows the aggregate node_B_1_aggr0 being taken offline:

      ```
      cluster_B::> storage aggregate offline -aggregate node_B_1_aggr0

      Aggregate offline successful on aggregate: node_B_1_aggr0
      ```

   b. Delete the aggregate: `storage aggregate delete -aggregate aggregate-name`

      You can destroy the plex when prompted.

      The following example shows the aggregate node_B_1_aggr0 being deleted.

      ```
      cluster_B::> storage aggregate delete -aggregate node_B_1_aggr0
      Warning: Are you sure you want to destroy aggregate "node_B_1_aggr0"?
      {y|n}: y
      [Job 123] Job succeeded: DONE

      cluster_B::>
      ```

5. Identify the MetroCluster FC DR group that need to be removed.

   In the following example the MetroCluster FC nodes are in DR Group '1', and this is the DR group that need to be removed.

```
cluster_B::> metrocluster node show

DR                                  Configuration  DR
Group Cluster Node                  State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        configured     enabled   normal
              node_A_2-FC        configured     enabled   normal
      cluster_B
              node_B_1-FC        configured     enabled   normal
              node_B_2-FC        configured     enabled   normal
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_3-IP        configured     enabled   normal
8 entries were displayed.

cluster_B::>
```

6. Move the cluster management LIF from a MetroCluster FC node to a MetroCluster IP node: `cluster_B::> network interface migrate -vserver svm-name -lif cluster_mgmt -destination-node node-in-metrocluster-ip-dr-group -destination-port available-port`
7. Change the home node and home port of the cluster management LIF: `cluster_B::> network interface modify -vserver svm-name -lif cluster_mgmt -service-policy default-management -home-node node-in-metrocluster-ip-dr-group -home-port lif-port`
8. Move epsilon from a MetroCluster FC node to a MetroCluster IP node:
   a. Identify which node currently has epsilon: `cluster show -fields epsilon`

   ```
   cluster_B::> cluster show -fields epsilon
   node             epsilon
   ---------------- -------
   node_A_1-FC      true
   node_A_2-FC      false
   node_A_1-IP      false
   node_A_2-IP      false
   4 entries were displayed.
   ```

   b. Set epsilon to false on the MetroCluster FC node (node_A_1-FC): `cluster modify -node fc-node -epsilon false`

c. Set epsilon to true on the MetroCluster IP node (node_A_1-IP): `cluster modify -node ip-node -epsilon true`

d. Verify that epsilon has moved to the correct node: `cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-FC      false
node_A_2-FC      false
node_A_1-IP      true
node_A_2-IP      false
4 entries were displayed.
```

9. On each cluster, remove the DR group containing the old nodes from the MetroCluster FC configuration.

   You must perform this step on both clusters, one at a time.

```
cluster_B::> metrocluster remove-dr-group -dr-group-id 1

Warning: Nodes in the DR group that are removed from the MetroCluster
         configuration will lose their disaster recovery protection.

         Local nodes "node_A_1-FC, node_A_2-FC" will be removed from the
         MetroCluster configuration. You must repeat the operation on
the
         partner cluster "cluster_B" to remove the remote nodes in the
DR group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the local and
partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the DR
group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed. Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in another DR
group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed ifthe preparation steps are not completed on
the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_B::>
```

10. Verify that the nodes are ready to be removed from the clusters.

    You must perform this step on both clusters.

    > At this point, the `metrocluster node show` command only shows the local MetroCluster FC nodes and no longer shows the nodes that are part of the partner cluster.

```
cluster_B::> metrocluster node show

DR                                  Configuration  DR
Group Cluster Node                  State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-FC        ready to configure
                                                   -         -
              node_A_2-FC        ready to configure
                                                   -         -
2     cluster_A
              node_A_3-IP        configured     enabled   normal
              node_A_4-IP        configured     enabled   normal
      cluster_B
              node_B_3-IP        configured     enabled   normal
              node_B_4-IP        configured     enabled   normal
6 entries were displayed.

cluster_B::>
```

11. Disable storage failover for the MetroCluster FC nodes.

    You must perform this step on each node.

```
cluster_A::> storage failover modify -node node_A_1-FC -enabled false
cluster_A::> storage failover modify -node node_A_2-FC -enabled false
cluster_A::>
```

12. Unjoin the MetroCluster FC nodes from the clusters: `cluster unjoin -node node-name`

    You must perform this step on each node.

```
cluster_A::> cluster unjoin -node node_A_1-FC

Warning: This command will remove node "node_A_1-FC"from the cluster.
You must
         remove the failover partner as well. After the node is removed,
erase
         its configuration and initialize all disks by usingthe "Clean
         configuration and initialize all disks (4)" option from the
boot menu.
Do you want to continue? {y|n}: y
[Job 553] Job is queued: Cluster remove-node of Node:node_A_1-FC with
UUID:6c87de7e-ff54-11e9-8371
[Job 553] Checking prerequisites
[Job 553] Cleaning cluster database
[Job 553] Job succeeded: Node remove succeeded
If applicable, also remove the node's HA partner, and then clean its
configuration and initialize all disks with the boot menu.
Run "debug vreport show" to address remaining aggregate or volume
issues.

cluster_B::>
```

13. Power down the MetroCluster FC controller modules and storage shelves.
14. Disconnect and remove the MetroCluster FC controller modules and storage shelves.

Completing the transition

To complete the transition you must verify the operation of the new MetroCluster IP configuration.

1. Verify the MetroCluster IP configuration.

   You must perform this step on each cluster.

   The following example shows the output for cluster_A.

```
cluster_A::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_A_1-IP          true    true          true
node_A_2-IP          true    true          false
2 entries were displayed.

cluster_A::>
```

The following example shows the output for cluster_B.

```
cluster_B::> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node_B_1-IP          true    true          true
node_B_2-IP          true    true          false
2 entries were displayed.

cluster_B::>
```

2. Enable cluster HA and storage failover.

   You must perform this step on each cluster.

3. Verify that cluster HA capability is enabled.

```
cluster_A::> cluster ha show
High Availability Configured: true

cluster_A::>


cluster_A::> storage  failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1-IP    node_A_2-IP    true     Connected to node_A_2-IP
node_A_2-IP    node_A_1-IP    true     Connected to node_A_1-IP
2 entries were displayed.

cluster_A::>
```

4. Disable MetroCluster transition mode.

   a. Change to the advanced privilege level: `set -privilege advanced`
   b. Disable transition mode:`metrocluster transition disable`
   c. Return to the admin privilege level: `set -privilege admin`

```
cluster_A::*> metrocluster transition disable

cluster_A::*>
```

5. Verify that transition is disabled:`metrocluster transition show-mode`

   You must perform these steps on both clusters.

```
cluster_A::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_A::>
```

```
cluster_B::> metrocluster transition show-mode
Transition Mode
--------------------------
not-enabled

cluster_B::>
```

Sending a custom AutoSupport message after maintenance

After completing the transition, you should send an AutoSupport message indicating the end of maintenance, so automatic case creation can resume.

1. To resume automatic support case generation, send an Autosupport message to indicate that the maintenance is complete.
   a. Issue the following command: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Repeat the command on the partner cluster.

Restoring Tiebreaker or Mediator monitoring

After completing the transition of the MetroCluster configuration, you can resume monitoring with the Tiebreaker or Mediator utility.

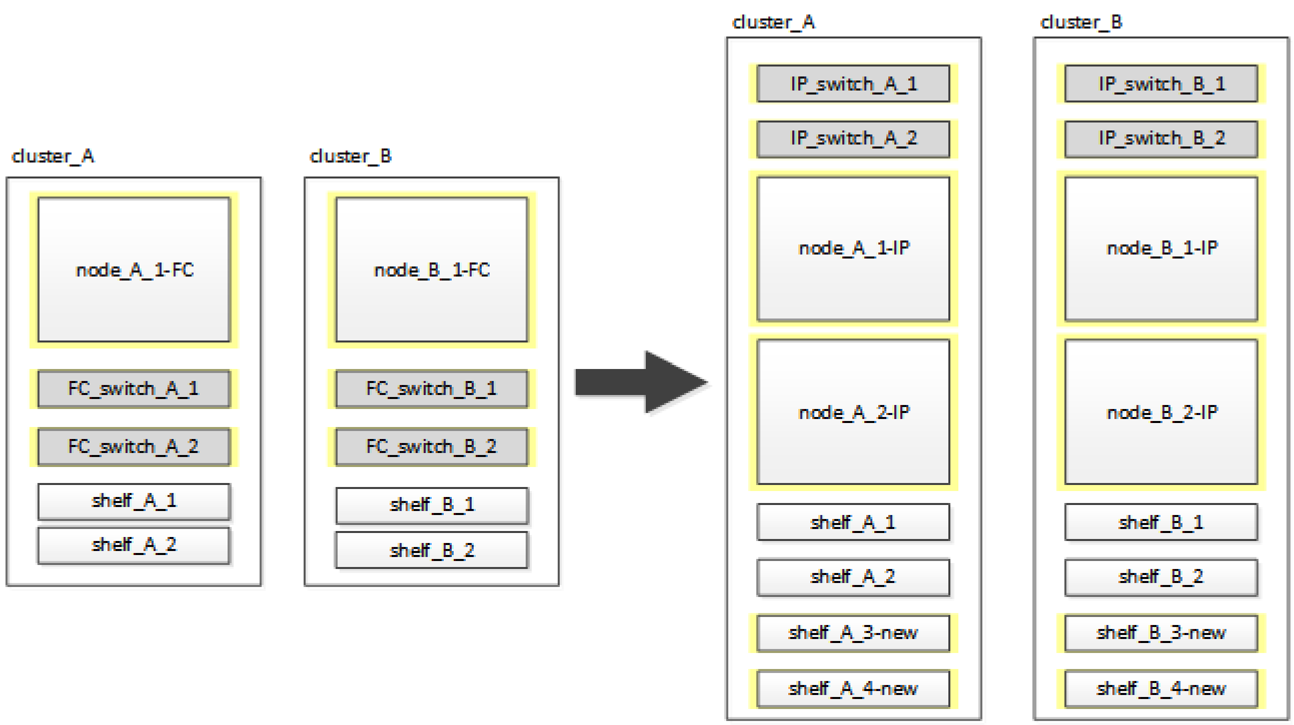
1. Use the appropriate procedure for your configuration.

If you are using…	Use this procedure
Tiebreaker	Adding MetroCluster configurations
Mediator	Configuring the ONTAP Mediator service from a MetroCluster IP configuration

Disruptively transitioning from a two-node MetroCluster FC to a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Starting with ONTAP 9.8, you can transition workloads and data from an existing two-node MetroCluster FC configuration to a new four-node MetroCluster IP configuration. Disk shelves from the MetroCluster FC nodes are moved to the IP nodes.

The following illustration provides a simplified view of the configuration before and after this transition procedure.



- This procedure is supported on systems running ONTAP 9.8 and later.
- This procedure is disruptive.
- This procedure applies only to a two-node MetroCluster FC configuration.

  If you have a four-node MetroCluster FC configuration, see Choosing your transition procedure.
- ADP is not supported on the four-node MetroCluster IP configuration created by this procedure.
- You must meet all requirements and follow all steps in the procedure.
- The existing storage shelves are moved to the new MetroCluster IP nodes.
- Additional storage shelves can be added to the configuration if necessary.

  See Drive shelf reuse and drive requirements for disruptive FC-to-IP transition.

Example naming in this procedure

This procedure uses example names throughout to identify the DR groups, nodes, and switches involved.

The nodes in the original configuration have the suffix -FC, indicating that they are in a fabric-attached or stretch MetroCluster configuration.

Components	cluster_A at site_A	cluster_B at site_B
dr_group_1-FC	• node_A_1-FC • shelf_A_1 • shelf_A_2	• node_B_1-FC • shelf_B_1 • shelf_B_2
dr_group_2-IP	• node_A_1-IP • node_A_2-IP • shelf_A_1 • shelf_A_2 • shelf_A_3-new • shelf_A_4-new	• node_B_1-IP • node_B_2-IP • shelf_B_1 • shelf_B_2 • shelf_B_3-new • shelf_B_4-new
Switches	• switch_A_1-FC • switch_A_2-FC • switch_A_1-IP • switch_A_2-IP	• switch_B_1-FC • switch_B_2-FC • switch_B_1-IP • switch_B_2-IP

Preparing for disruptive FC-to-IP transition

General requirements for disruptive FC-to-IP transition

Before starting the transition process, you must make sure the configuration meets the requirements.

The existing MetroCluster FC configuration must meet the following requirements:

- It must be a two-node configuration and all nodes must be running ONTAP 9.8 or later.

  It can be a two-node fabric-attached or stretched MetroCluster.

- It must meet all requirements and cabling as described in the *MetroCluster Installation and Configuration Guides*.

  Fabric-attached MetroCluster installation and configuration

  Stretch MetroCluster installation and configuration

- It cannot be configured with NetApp Storage Encryption (NSE).
- The MDV volumes cannot be encrypted.

You must have remote console access for all six nodes from either MetroCluster site or plan for travel between the sites as required by the procedure.

Drive shelf reuse and drive requirements for disruptive FC-to-IP transition

You must ensure that adequate spare drives and root aggregate space is available on the storage shelves.

Reusing the existing storage shelves

When using this procedure, the existing storage shelves are retained for use by the new configuration. When node_A_1-FC and node_B_1-FC are removed, the existing drive shelves are connected to node_A_1-IP and node_A_2-IP on cluster_A and to node_B_1-IP and node_B_2-IP on cluster_B.

- The existing storage shelves (those attached to node_A_1-FC and node_B_1-FC) must be supported by the new platform models.

  If the existing shelves are not supported by the new platform models, see Disruptively transitioning when existing shelves are not supported on new controllers (ONTAP 9.8 and later).

  NetApp Hardware Universe

- You must ensure you don’t exceed the platform limits for drives, etc.

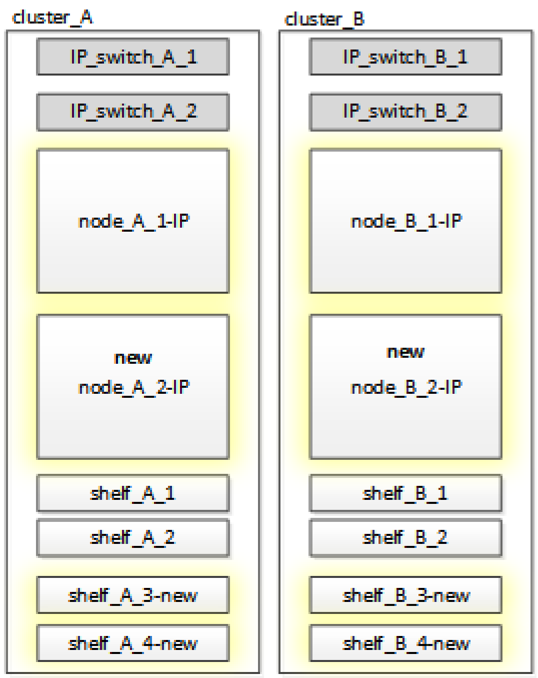
  HWU link

Storage requirements for the additional controllers

Additional storage must be added, if necessary, to accommodate the two additional controllers (node_A_2-IP and node_B_2-ip), because the configuration is changing from a two-node to a four-node arrangement.

- Depending on the spare drives available in the existing shelves, additional drives must be added to accommodate the additional controllers in the configuration.

  This might require additional storage shelves, as shown in the following illustration.



You need to have additional 14 - 18 drives each for the third and fourth controllers (node_A_2-IP and node_B_2-IP):

- Three pool0 drives
- Three pool1 drives
- Two spare drives
- Six to ten drives for the system volume

- You must ensure that the configuration, including the new nodes, does not exceed the platform limits for the configuration, including drive count, root aggregate size capacity, etc.

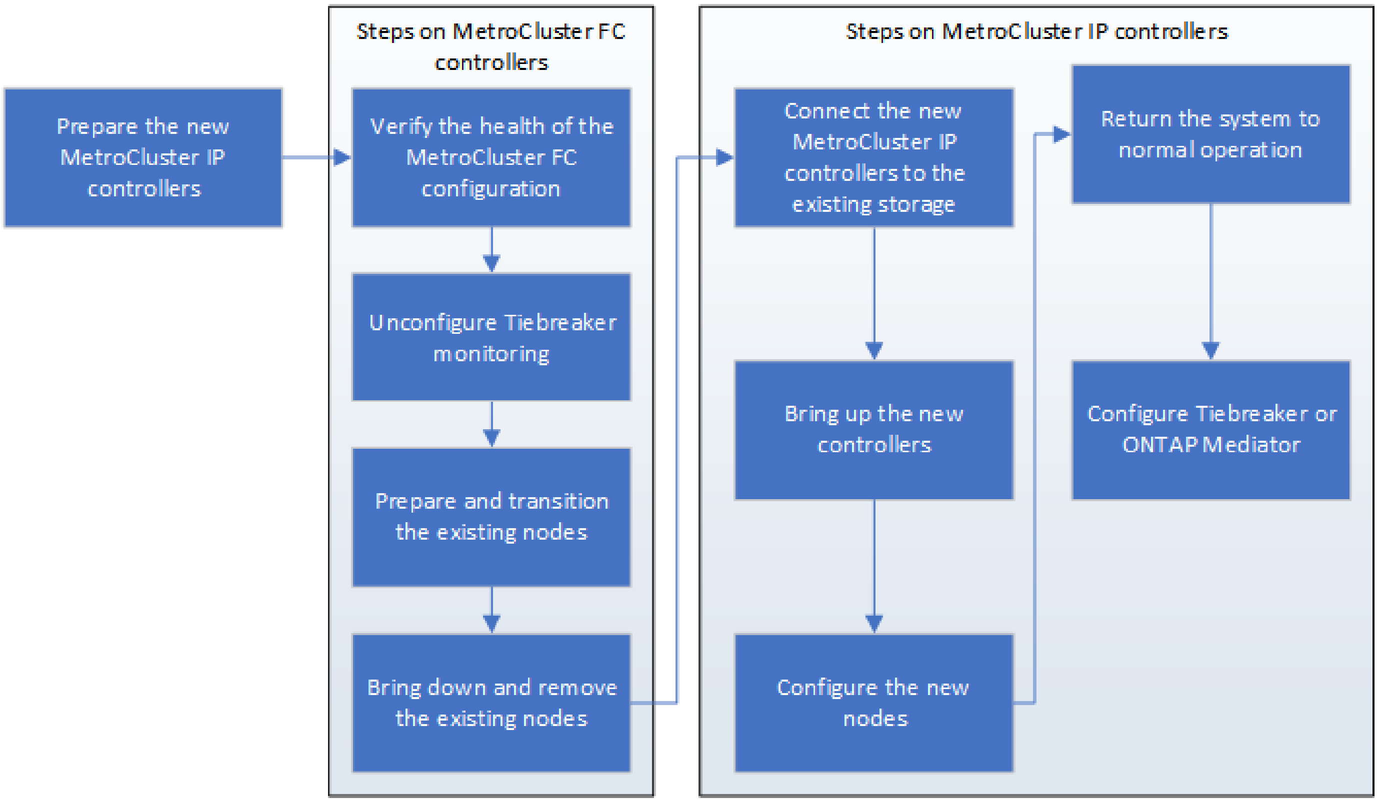
  This information is available for each platform model at *NetApp Hardware Universe*.

  NetApp Hardware Universe

Workflow for disruptive transition

You must follow the specific workflow to ensure a successful transition.

As you prepare for the transition, plan for travel between the sites. Note that after the remote nodes are racked and cabled, you need serial terminal access to the nodes. Service Processor access is not be available until the nodes are configured.



Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes

You must adjust the port and LIF configuration of the MetroCluster FC node so it is compatible with that of the MetroCluster IP node that will replace it.

When the new nodes are first booted during the upgrade process, each node uses the most recent configuration of the node it is replacing. When you boot node_A_1-IP, ONTAP attempts to host LIFs on the same ports that were used on node_A_1-FC.

During the transition procedure, you will perform steps on both the old and new nodes to ensure correct cluster, management, and data LIF configuration.

1. Identify any conflicts between the existing MetroCluster FC port usage and the port usage for the MetroCluster IP interfaces on the new nodes.

   You must identify the MetroCluster IP ports on the new MetroCluster IP controllers using the table below. Then check and record if any data LIFs or cluster LIFs exist on those ports on the MetroCluster FC nodes.

   These conflicting data LIFs or cluster LIFs on the MetroCluster FC nodes will be moved at the appropriate step in the transition procedure.

   > ⓘ On the AFF A220 and FAS2750 systems, the MetroCluster IP physical ports are also used as cluster interfaces. If the new MetroCluster IP nodes are AFF A220 or FAS2750 systems, existing cluster LIFs do not need to be moved.

   The following table shows the MetroCluster IP ports by platform model. You can ignore the VLAN ID column.

Platform model	MetroCluster IP port	VLAN ID	
AFF A800	e0b	Not used	
	e1b		
AFF A700 and FAS9000	e5a		
	e5b		
AFF A320	e0g		
	e0h		
AFF A300 and FAS8200	e1a		
	e1b		
AFF A220 and FAS2750	e0a	10	On these systems, these physical ports are also used as cluster interfaces.
	e0b	20	
AFF A250 and FAS500f	e0c	10	
	e0d	20	

You can fill in the following table and refer to it later in the transition procedure.

Ports	Corresponding MetroCluster IP interface ports (from table above)	Conflicting LIFs on these ports on the MetroCluster FC nodes
First MetroCluster IP port on node_A_1-FC		
Second MetroCluster IP port on node_A_1-FC		
First MetroCluster IP port on node_B_1-FC		
Second MetroCluster IP port on node_B_1-FC		

2. Determine what physical ports are available on the new controllers and what LIFs can be hosted on the ports.

The controller's port usage depends on the platform model and IP switch model you will use in the MetroCluster IP configuration. You can gather the port usage of the new platforms from the *NetApp Hardware Universe*.

NetApp Hardware Universe

3. If desired, record the port information for node_A_1-FC and node_A_1-IP.

   You will refer to the table as you carry out the transition procedure.

   In the columns for node_A_1-IP, add the physical ports for the new controller module and plan the IPspaces and broadcast domains for the new node.

	node_A_1-FC			**node_A_1-IP**		
LIF	**Ports**	**IPspaces**	**Broadcast domains**	**Ports**	**IPspaces**	**Broadcast domains**
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Node management						
Cluster management						
Data 1						
Data 2						
Data 3						
Data 4						
SAN						
Intercluster port						

4. If desired, record all the port information for node_B_1-FC.

   You will refer to the table as you carry out the upgrade procedure.

   In the columns for node_B_1-IP, add the physical ports for the new controller module and plan the LIF port usage, IPspaces and broadcast domains for the new node.

	node_B_1-FC			**node_B_1-IP**		
LIF	**Physical ports**	**IPspaces**	**Broadcast domains**	**Physical ports**	**IPspaces**	**Broadcast domains**
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Node management						
Cluster management						
Data 1						
Data 2						
Data 3						
Data 4						
SAN						
Intercluster port						

Preparing the MetroCluster IP controllers

You must prepare the four new MetroCluster IP nodes and install the correct ONTAP version.

This task must be performed on each of the new nodes:

- node_A_1-IP
- node_A_2-IP
- node_B_1-IP
- node_B_2-IP

The nodes should be connected to any **new** storage shelves. They must **not** be connected to the existing storage shelves containing data.

These steps can be performed now, or later in the procedure when the controllers and shelves are racked. In any case, you must make sure you clear the configuration and prepare the nodes **before** connecting them to the existing storage shelves and **before** making any configuration changes to the MetroCluster FC nodes.

> Do not perform these steps with the MetroCluster IP controllers connected to the existing storage shelves that were connected to the MetroCluster FC controllers.

In these steps, you clear the configuration on the nodes and clear the mailbox region on new drives.

1. Connect the controller modules to the new storage shelves.
2. In Maintenance mode, display the HA state of the controller module and chassis: `ha-config show`

   The HA state for all components should be mccip.

3. If the displayed system state of the controller or chassis is not correct, set the HA state: `ha-config modify controller mccip``ha-config modify chassis mccip`
4. Exit Maintenance mode: `halt`

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

5. Repeat the following substeps on all four nodes to clear the configuration:
   a. Set the environmental variables to default values: `set-defaults`
   b. Save the environment: `saveenv``bye`
6. Repeat the following substeps to boot all four nodes using the 9a option on the boot menu.
   a. At the LOADER prompt, launch the boot menu: `boot_ontap menu`
   b. At the boot menu, select option **9a** to reboot the controller.
7. Boot each of the four nodes to Maintenance mode using option **5** on the boot menu.
8. Record the system ID and from each of the four nodes: `sysconfig`
9. Repeat the following steps on node_A_1-IP and node_B_1-IP.
   a. Assign ownership of all disks local to each site: `disk assign adapter.xx.*`
   b. Repeat the previous step for each HBA with attached drive shelves on node_A_1-IP and node_B_1-IP.
10. Repeat the following steps on node_A_1-IP and node_B_1-IP to clear the mailbox region on each local disk.
    a. Destroy the mailbox region on each disk: `mailbox destroy local``mailbox destroy partner`
11. Halt all four controllers: `halt`
12. On each controller, display the boot menu: `boot_ontap menu`
13. On each of the four controllers, clear the configuration: `wipeconfig`

    When the wipeconfig operation completes, the node automatically returns to the boot menu.

14. Repeat the following substeps to again boot all four nodes using the 9a option on the boot menu.
    a. At the LOADER prompt, launch the boot menu: `boot_ontap menu`

b. At the boot menu, select option **9a** to reboot the controller.
c. Let the controller module complete booting before moving to the next controller module.

After 9a completes, the nodes automatically return to the boot menu.

15. Power off the controllers.

Verifying the health of the MetroCluster FC configuration

You must verify the health and connectivity of the MetroCluster FC configuration prior to performing the transition

This task is performed on the MetroCluster FC configuration.

1. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:`node run -node node-name sysconfig -a`
   b. Check for any health alerts on both clusters: `system health alert show`
   c. Confirm the MetroCluster configuration and that the operational mode is normal: `metrocluster show`
   d. Perform a MetroCluster check: `metrocluster check run`
   e. Display the results of the MetroCluster check: `metrocluster check show`
   f. Check for any health alerts on the switches (if present): `storage switch show`
   g. Run Config Advisor.

      NetApp Downloads: Config Advisor

   h. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.
2. Verify that the nodes are in non-HA mode: `storage failover show`

Removing the existing configuration from the Tiebreaker or other monitoring software

If the existing configuration is monitored with the MetroCluster Tiebreaker configuration or other third-party applications (for example, ClusterLion) that can initiate a switchover, you must remove the MetroCluster configuration from the Tiebreaker or other software prior to transition.

1. Remove the existing MetroCluster configuration from the Tiebreaker software.

   Removing MetroCluster configurations

2. Remove the existing MetroCluster configuration from any third-party application that can initiate switchover.

   Refer to the documentation for the application.

Transitioning the MetroCluster FC nodes

You must gather information from the existing MetroCluster FC nodes, send an autosupport message announcing the start of maintenance, and transition the nodes.

Gathering information from the existing controller modules before the transition

Before transitioning, you must gather information for each of the nodes.

This task is performed on the existing nodes:

- node_A_1-FC
- node_B_1-FC

1. Gather the output for the commands in the following table.

Category	Commands	Notes
License	system license show	
Shelves and numbers of disks in each shelf and flash storage details and memory and NVRAM and and network cards	system node run -node node_name sysconfig	
Cluster network and node management LIFs	system node run -node node_name sysconfig network interface show -role "cluster,node-mgmt,data"	
SVM information	vserver show	
Protocol information	nfs show iscsi show cifs show	
Physical ports	network port show -node node_name -type physical network port show	
Failover Groups	network interface failover-groups show -vserver vserver_name	Record the names and ports of failover groups that are not clusterwide.
VLAN configuration	network port vlan show -node node_name	Record each network port and VLAN ID pairing.
Interface group configuration	network port ifgrp show -node node_name -instance	Record the names of the interface groups and the ports assigned to them.
Broadcast domains	network port broadcast-domain show	
IPspace	network ipspace show	
Volume info	volume show and volume show -fields encrypt	
Aggregate Info	storage aggregate show and storage aggr encryption show andstorage aggregate object-store show	

Category	Commands	Notes
Disk ownership information	storage aggregate show and storage aggr encryption show andstorage aggregate object-store show	
Encryption	storage failover mailbox-disk show and security key-manager backup show	Also preserve the passphrase used to enable key-manager. In the case of external key-manager you will need the authentication information for the client and server.
Encryption	security key-manager show	
Encryption	security key-manager external show	
Encryption	systemshell local kenv kmip.init.ipaddr ip-address	
Encryption	systemshell local kenv kmip.init.netmask netmask	
Encryption	systemshell local kenv kmip.init.gateway gateway	
Encryption	systemshell local kenv kmip.init.interface interface	

Sending a custom AutoSupport message prior to maintenance

Before performing the maintenance, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. This prevents them from opening a case on the assumption that a disruption has occurred.

This task must be performed on each MetroCluster site.

1. To prevent automatic support case generation, send an Autosupport message to indicate maintenance is underway.
   a. Issue the following command: `system node autosupport invoke -node * -type all -message MAINT=maintenance-window-in-hours`

      maintenance-window-in-hours specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:`system node autosupport invoke -node * -type all -message MAINT=end`

   b. Repeat the command on the partner cluster.

Transitioning, shutting down, and removing the MetroCluster FC nodes

In addition to issuing commands on the MetroCluster FC nodes, this task includes physical uncabling and removal of the controller modules at each site.

This task must be performed on each of the old nodes:

- node_A_1-FC
- node_B_1-FC

1. Stop all client traffic.
2. On either of the MetroCluster FC nodes, for example node_A_1-FC, enable transition.
   a. Set the advanced privilege level: `set -priv advanced`
   b. Enable transition: `metrocluster transition enable -transition-mode disruptive`
   c. Return to admin mode: `set -priv admin`
3. Unmirror the root aggregate by deleting the remote plex of the root aggregates.
   a. Identify the root aggregates: `storage aggregate show -root true`
   b. Display the pool1 aggregates: `storage aggregate plex show -pool 1`
   c. Delete the local plex of the root aggregate: `aggr plex delete aggr-name -plex plex-name`
   d. Offline the remote plex of the root aggregate: `aggr plex offline root-aggregate -plex remote-plex-for-root-aggregate`

      For example:

      ```
      # aggr plex offline aggr0_node_A_1-FC_01 -plex plex4
      ```
4. Confirm the mailbox count, disk autoassign, and transition mode before proceeding using the following commands on each controller:
   a. Set the advanced privilege level: `set -priv advanced`
   b. Confirm that only three mailbox drives are shown for each controller module: `storage failover mailbox-disk show`
   c. Return to admin mode: `set -priv admin`
   d. Confirm that the transition mode is disruptive: metrocluster transition show
5. Check for any broken disks: `disk show -broken`
6. Remove or replace any broken disks
7. Confirm aggregates are healthy using the following commands on node_A_1-FC and node_B_1-FC:`storage aggregate showstorage aggregate plex show`

   The storage aggregate show command indicates that the root aggregate is unmirrored.
8. Check for any VLANs or interface groups: `network port ifgrp show``network port vlan show`

   If none are present, skip the following two steps.
9. Display the list of LIfs using VLANs or ifgrps: `network interface show -fields home-port,curr-port``network port show -type if-group | vlan`

10. Remove any VLANs and interface groups.

    You must perform these steps for all LIFs in all SVMs, including those SVMs with the -mc suffix.

    a. Move any LIFs using the VLANs or interface groups to an available port: `network interface modify -vserver vserver-name -lif lif_name -home- port port`
    b. Display the LIFs that are not on their home ports: `network interface show -is-home false`
    c. Revert all LIFs to their respective home ports: `network interface revert -vserver vserver_name -lif lif_name`
    d. Verify that all LIFs are on their home ports: `network interface show -is-home false`

       No LIFs should appear in the output.

    e. Remove VLAN and ifgrp ports from broadcast domain:: `network port broadcast-domain remove-ports -ipspace ipspace -broadcast-domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`
    f. Verify that all the vlan and ifgrp ports are not assigned to a broadcast domain: `network port show -type if-group | vlan`
    g. Delete all VLANs: `network port vlan delete -node nodename -vlan-name vlan-name`
    h. Delete interface groups: `network port ifgrp delete -node nodename -ifgrp ifgrp-name`
11. Move any LIFs as required to resolve conflicts with the MetroCluster IP interface ports.

    You must move the LIFs identified in step 1 of Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes.

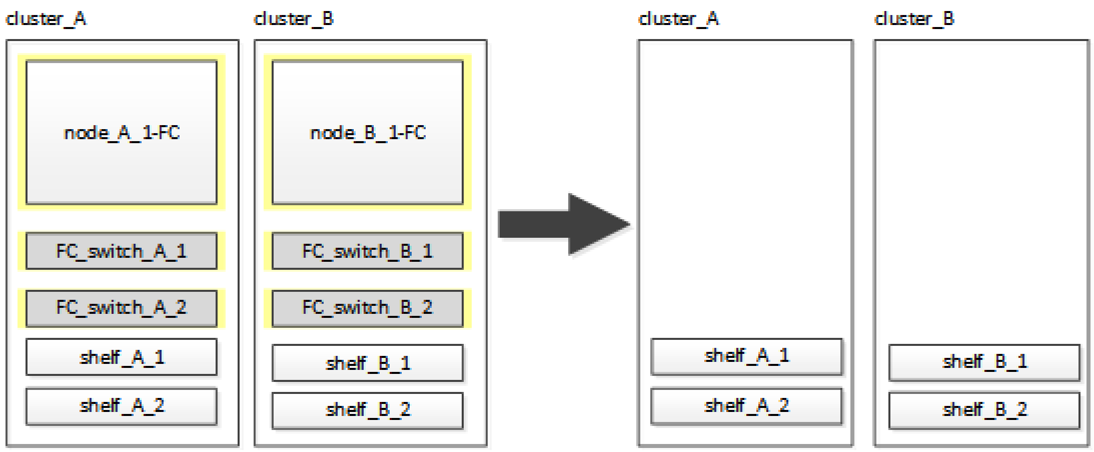
    a. Move any LIFs hosted on the desired port to another port: `network interface modify -lif lifname -vserver vserver-name -home-port new-homeport``network interface revert -lif lifname -vserver vservername`
    b. If necessary, move the destination port to an appropriate IPspace and broadcast domain. `network port broadcast-domain remove-ports -ipspace current-ipspace -broadcast -domain current-broadcast-domain -ports controller-name:current-port``network port broadcast-domain add-ports -ipspace new-ipspace -broadcast-domain new-broadcast-domain -ports controller-name:new-port`
12. Halt the MetroCluster FC controllers (node_A_1-FC and node_B_1-FC): `system node halt`
13. At the LOADER prompt, synchronize the hardware clocks between the FC and IP controller modules.
    a. On the old MetroCluster FC node (node_A_1-FC), display the date: `show date`
    b. On the new MetroCluster IP controllers (node_A_1-IP and node_B_1-IP), set the date shown on original controller: `set date mm/dd/yy`
    c. On the new MetroCluster IP controllers (node_A_1-IP and node_B_1-IP), verify the date: `show date`
14. Halt and power off the MetroCluster FC controller modules (node_A_1-FC and node_B_1-FC), FC-to-SAS bridges (if present), FC switches (if present) and each storage shelf connected to these nodes.

15. Disconnect the shelves from the MetroCluster FC controllers and document which shelves are local storage to each cluster.

    If the configuration uses FC-to-SAS bridges or FC back-end switches, disconnect and remove them.

16. In Maintenance mode on the MetroCluster FC nodes (node_A_1-FC and node_B_1-FC), confirm no disks are connected: `disk show -v`
17. Power down and remove the MetroCluster FC nodes.

At this point, the MetroCluster FC controllers have been removed and the shelves are disconnected from all controllers.



Connecting the MetroCluster IP controller modules

You must add the four new controller modules and any additional storage shelves to the configuration. The new controller modules are added two-at-a-time.

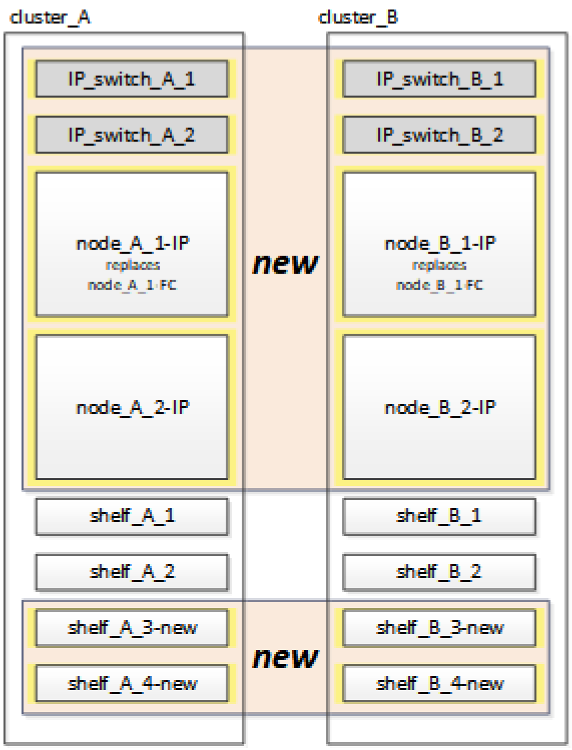
Setting up the new controllers

You must rack and cable the new MetroCluster IP controllers to the storage shelves previously connected to the MetroCluster FC controllers.

These steps must be performed on each of the MetroCluster IP nodes.

- node_A_1-IP
- node_A_2-IP
- node_B_1-IP
- node_B_2-IP

In the following example, two additional storage shelves are added at each site to provide storage to accommodate the new controller modules.



1. Plan out the positioning of the new controller modules and storage shelves as needed.

   The rack space depends on the platform model of the controller modules, the switch types, and the number of storage shelves in your configuration.

2. Properly ground yourself.
3. Rack the new equipment: controllers, storage shelves, and IP switches.

   Do not cable the storage shelves or IP switches at this time.

4. Connect the power cables and management console connection to the controllers.
5. Verify that all storage shelves are powered off.
6. Verify that no drives are connected by performing the following steps on all four nodes:
   a. At the LOADER prompt, launch the boot menu: `boot_ontap maint`
   b. Verify that no drives are connected: `disk show -v`

      The output should show no drives.

   c. Halt the node: `halt`
7. Boot all four nodes using the 9a option on the boot menu.
   a. At the LOADER prompt, launch the boot menu: `boot_ontap menu`
   b. At the boot menu, select option **9a** to reboot the controller.
   c. Let the controller module complete booting before moving to the next controller module.

   After 9a completes, the nodes automatically return to the boot menu.

8. Cable the storage shelves.

Refer to the controller installation and setup procedures for your model for cabling information.

AFF and FAS Documentation Center

9. Cable the controllers to the IP switches as described in the *MetroCluster IP Installation and Configuration Guide*.

   MetroCluster IP installation and configuration

   - Cabling the IP switches

10. Prepare the IP switches for the application of the new RCF files.

    Follow the steps in the section for your switch vendor from the *MetroCluster IP Installation and Configuration Guide*.

    MetroCluster IP installation and configuration

    - Resetting the Broadcom IP switch to factory defaults
    - Resetting the Cisco IP switch to factory defaults

11. Download and install the RCF files.

    Follow the steps in the section for your switch vendor from the MetroCluster IP installation and configuration.

    - Downloading and installing the Broadcom RCF files
    - Downloading and installing the Cisco IP RCF files

12. Turn on power to the first new controller (node_A_1-IP) and press Ctrl-C to interrupt the boot process and display the LOADER prompt.
13. Boot the controller to Maintenance mode: `boot_ontap_maint`
14. Display the system ID for the controller: `sysconfig -v`
15. Confirm that the shelves from the existing configuration are visible from the new MetroCluster IP node: `storage show shelf``disk show -v`
16. Halt the node: `halt`
17. Repeat the preceding steps on the other node at the partner site (site_B).

Connecting and booting up node_A_1-IP and node_B_1-IP

After connecting the MetroCluster IP controllers and IP switches, you transition and boot up node_A_1-IP and node_B_1-IP.

Bringing up node_A_1-IP

You must boot the node with the correct transition option.

1. Boot node_A_1-IP to the boot menu: `boot_ontap menu`
2. Issue the following command at the boot menu prompt to initiate transition: `boot_after_mcc_transition`

- This command reassigns all the disks owned by node_A_1-FC to node_A_1-IP.
    - node_A_1-FC disks are assigned to node_A_1-IP
    - node_B_1-FC disks are assigned to node_B_1-IP
- The command also automatically makes other required system ID reassignments so the MetroCluster IP nodes can boot to the ONTAP prompt.
- If the boot_after_mcc_transition command fails for any reason, it should be re-run from the boot menu. **Note:**
- If the following prompt is displayed, enter Ctrl-C to continue. Checking MCC DR state… [enter Ctrl-C(resume), S(status), L(link)]_
- If the root volume was encrypted, the node halts with the following message. Halting the system, because root volume is encrypted (NetApp Volume Encryption) and the key import failed. If this cluster is configured with external (KMIP) key-manager, check the health of the key servers.

```
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)?
`boot_after_mcc_transition`
This will replace all flash-based configuration with the last backup to
disks. Are you sure you want to continue?: yes

MetroCluster Transition: Name of the MetroCluster FC node: `node_A_1-FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of MetroCluster
FC node node_A_1-FC: `systemID-of-node_B_1-FC`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
MetroCluster Transition: Disaster Recovery partner sysid of local
MetroCluster IP node: `systemID-of-node_B_1-IP`
MetroCluster Transition: Please confirm if this is the correct value
[yes|no]:? y
```

3. If data volumes are encrypted, restore the keys using the correct command for your key management configuration.

If you are using…	Use this command…
Onboard key management	security key-manager onboard sync For more information, see Restoring onboard key management encryption keys.
External key management	security key-manager key query -node node-name For more information, see Restoring external key management encryption keys. +

4. If the root volume is encrypted, use the procedure in Recovering key management if the root volume is encrypted.

Recovering key management if the root volume is encrypted

If the root volume is encrypted, you must use special boot commands to restore the key management.

You must have the passphrases gathered earlier.

1. If onboard key management is used, perform the following substeps to restore the configuration.
   a. From the LOADER prompt, display the boot menu: `boot_ontap menu`
   b. Select option (10) Set onboard key management recovery secrets from the boot menu.

      Respond as appropriate to the prompts:

```
This option must be used only in disaster recovery procedures. Are
you sure? (y or n): `y`
Enter the passphrase for onboard key management: `passphrase`
Enter the passphrase again to confirm:`passphrase`

Enter the backup data:`backup-key`
```

      The system boots to the boot menu.

   c. Enter option `6` at the boot menu.

      Respond as appropriate to the prompts:

```
This will replace all flash-based configuration with the last backup
to
disks. Are you sure you want to continue?: y

Following this, the system will reboot a few times and the following
prompt will be available continue by saying y

WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
```

After the reboots, the system will be at the LOADER prompt.

d. From the LOADER prompt, display the boot menu: `boot_ontap menu`

e. Again elect option (10) Set onboard key management recovery secrets from the boot menu.

Respond as appropriate to the prompts:

```
This option must be used only in disaster recovery procedures. Are
you sure? (y or n): `y`
Enter the passphrase for onboard key management: `passphrase`
Enter the passphrase again to confirm:`passphrase`

Enter the backup data:`backup-key`
```

The system boots to the boot menu.

f. Enter option `1` at the boot menu.

If the following prompt is displayed, you can enter Ctrl+C to resume the process. *Checking MCC DR state… [enter Ctrl-C(resume), S(status), L(link)]*

The system boots to the ONTAP prompt.

g. Restore the onboard key management: `security key-manager onboard sync`

Respond as appropriate to the prompts, using the passphrase you collected earlier:

```
cluster_A::> security key-manager onboard sync
Enter the cluster-wide passphrase for onboard key management in
Vserver "cluster_A":: passphrase
```

2. If external key management is used, perform the following substeps to restore the configuration.

a. Set the required bootargs: `setenv bootarg.kmip.init.ipaddr ip-addresssetenv bootarg.kmip.init.netmask netmasksetenv bootarg.kmip.init.gateway gateway-`

address``setenv bootarg.kmip.init.interface interface-id

b. From the LOADER prompt, display the boot menu: `boot_ontap menu`
c. Select option (11) Configure node for external key management from the boot menu.

   The system boots to the boot menu.

d. Enter option `6` at the boot menu.

   The system boots multiple times. You can respond affirmatively when prompted to continue the boot process.

   After the reboots, the system will be at the LOADER prompt.

e. Set the required bootargs: `setenv bootarg.kmip.init.ipaddr ip-addresssetenv bootarg.kmip.init.netmask netmasksetenv bootarg.kmip.init.gateway gateway-address``setenv bootarg.kmip.init.interface interface-id`
f. From the LOADER prompt, display the boot menu: `boot_ontap menu`
g. Again select option (11) Configure node for external key management from the boot menu and respond to the prompts as required.

   The system boots to the boot menu.

h. Restore the external key management: `security key-manager external restore`

Creating the network configuration

You must create a network configuration that matches the configuration on the FC nodes. This is because the MetroCluster IP node replays the same configuration when it boots, which means that when node_A_1-IP and node_B_1-IP boot, ONTAP will try to host LIFs on the same ports that were used on node_A_1-FC and node_B_1-FC respectively.

As you create the network configuration, use the plan made in Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes to assist you.

NOTE:

Additional configuration may be needed to bring up data LIFs after the MetroCluster IP nodes have been configured.

1. Verify that all cluster ports are in the appropriate broadcast domain:

   The cluster IPspace and cluster broadcast domain are required in order to create cluster LIFs

   a. View the IP spaces: `network ipspace show`
   b. Create IP spaces and assign cluster ports as needed.

      Configuring IPspaces (cluster administrators only)

   c. View the broadcast domains: `network port broadcast-domain show`
   d. Add any cluster ports to a broadcast domain as needed.

Adding or removing ports from a broadcast domain

e. Recreate VLANs and interface groups as needed.

VLAN and interface group membership might be different than that of the old node.

Creating a VLAN

Combining physical ports to create interface groups

2. Verify that MTU settings are set correctly for the ports and broadcast domain and make changes using the following commands: `network port broadcast-domain show``network port broadcast-domain modify -broadcast- domain bcastdomainname -mtu mtu`

Setting up cluster ports and cluster LIFs

You must set up cluster ports and LIFs. The following steps need to be performed on the site A nodes which were booted up with root aggregates.

1. Identify the list of LIFs using the desired Cluster port: `network interface show -curr-port portname``network interface show -home-port portname`
2. For each cluster port, change the home port of any of the LIFs on that port to another port,
   a. Enter advanced privilege mode and enter y when prompted to continue: `set priv advanced`
   b. If the LIF being modified is a data LIF: `vserver config override -command "network interface modify -lif lifname -vserver vservername -home-port new-datahomeport`
   c. If the LIF is not a data LIF: `network interface modify -lif lifname -vserver vservername -home-port new-datahomeport`
   d. Revert the modified LIFs to their home port: `network interface revert * -vserver vserver_name`
   e. Verify that there are no LIFs on the cluster port: `network interface show -curr-port portname``network interface show -home-port portname`
   f. Remove the port from the current broadcast domain: `network port broadcast-domain remove-ports -ipspace ipspacename -broadcast-domain bcastdomainname -ports node_name:port_name`
   g. Add the port to the cluster IPspace and broadcast domain: `network port broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports node_name:port_name`
   h. Verify that the port's role has changed: `network port show`
   i. Repeat these substeps for each cluster port.
   j. Return to admin mode: `set priv admin`
3. Create cluster LIFs on the new cluster ports:
   a. For autoconfiguration using link-local address for cluster LIF, use the following command: `network interface create -vserver Cluster -lif cluster_lifname -service-policy default-cluster -home-node a1name -home-port clusterport -auto true`

b. To assign static IP address for the cluster LIF, use the following command: `network interface create -vserver Cluster -lif cluster_lifname -service-policy default-cluster -home-node a1name -home-port clusterport -address ip-address -netmask netmask -status-admin up`

Verifying LIF configuration

The node management LIF, cluster management LIF and intercluster LIF will still be present after the storage movement from the old controller. If necessary, you must move LIFs to appropriate ports.

1. Verify if the management LIF and cluster management LIFs are on desired port already: `network interface show -service-policy default-management``network interface show -service-policy default-intercluster`

   If the LIFs are on the desired ports, you can skip the rest of the steps in this task and proceed to the next task.

2. For each node, cluster management, or intercluster LIFs are not on the desired port, change the home port of any of the LIFs on that port to another port,

   a. Repurpose the desired port by moving any LIFs hosted on desired port to another port using `vserver config override -command "network interface modify -lif <lifname> -vserver <vservername> -home-port <new-datahomeport>`

   b. Revert the modified LIFs to their new home port: `vserver config override -command "network interface revert -lif <lifname> -vserver <vservername>"`

   c. If the desired port is not in the right IPspace and broadcast domain, remove the port from the current IPspace and broadcast domain: `network port broadcast-domain remove-ports -ipspace <current-ipspace> -broadcast-domain <current-broadcast-domain> -ports <controller-name:current-port>`

   d. Move the desired port to the right IPspace and broadcast domain`network port broadcast-domain add-ports -ipspace <new-ipspace> -broadcast-domain <new-broadcast-domain> -ports <controller-name:new-port>`

   e. Verify that the port’s role has changed: `network port show`

   f. Repeat these substeps for each port.

3. Move node, cluster management LIFs and intercluster LIF to the desired port using the following commands:

   a. Change the LIF’s home port: `network interface modify -vserver vserver -lif node_mgmt -home-port port -home-node homenode`

   b. Revert the LIF to its new home port: `network interface revert -lif node_mgmt -vserver vservername`

   c. Change the cluster management LIF’s home port:`network interface modify -vserver vserver -lif cluster-mgmt-LIF-name -home-port port -home-node homenode`

   d. Revert the cluster management LIF to its new home port: `network interface revert -lif cluster-mgmt-LIF-name -vserver vservername`

   e. Change the intercluster LIF’s home port:`network interface modify -vserver vserver -lif intercluster-lif-name -home-node nodename -home-port port`

f. Revert the intercluster LIF to its new home port: `network interface revert -lifintercluster-lif-name -vserver vservername`

Bringing up node_A_2-IP and node_B_2-IP

You must bring up and configure the new MetroCluster IP node at each site, creating an HA pair in each site.

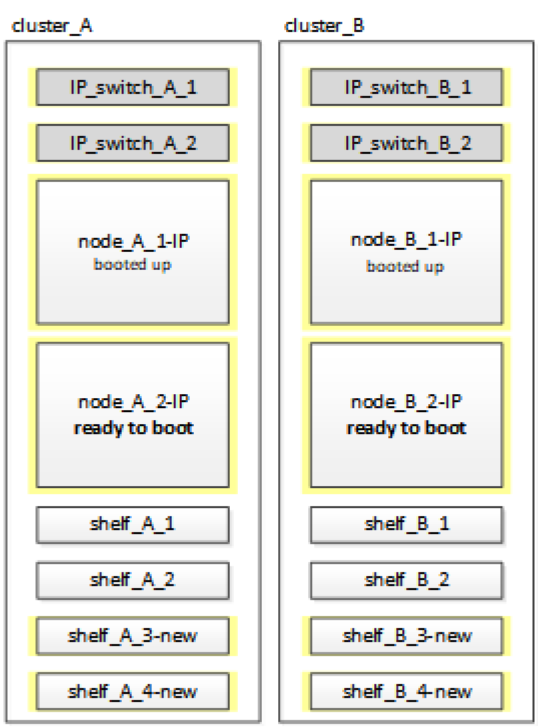
Bringing up node_A_2-IP and node_B_2-IP

You must boot the new controller modules one at a time using the correct option at the boot menu.

In these steps, you boot up the two brand new nodes, expanding what had been a two-node configuration into a four-node configuration.

These steps are performed on the following nodes:

- node_A_2-IP
- node_B_2-IP



1. Boot the new nodes using boot option `9c`.

```
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)? 9c
```

The node initializes and boots to the node setup wizard, similar to the following.

```
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. .
.
.
```

If option `9c` does not succeed, take the following steps to avoid possible data loss:

- Do not attempt to run option 9a.
- Physically disconnect the existing shelves that contain data from the original MetroCluster FC configuration (shelf_A_1, shelf_A_2, shelf_B_1, shelf_B_2).
- Contact technical support, referencing the KB article MetroCluster FC to IP transition - Option 9c Failing.

  NetApp Support

2. Enable the AutoSupport tool by following the directions provided by the wizard.
3. Respond to the prompts to configure the node management interface.

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Verify that the storage failover mode is set to HA: `storage failover show -fields mode`

   If the mode is not HA, set it: `storage failover modify -mode ha -node localhost`

You must then reboot the node for the change to take effect.

5. List the ports in the cluster:`network port show`

   For complete command syntax, see the man page.

   The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                                    Speed
(Mbps)
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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

6. Exit the Node Setup wizard: `exit`
7. Log into the admin account using the admin user name.
8. Join the existing cluster using the Cluster Setup wizard.

```
:> 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}:
join
```

9. After you complete the Cluster Setup wizard and it exits, verify that the cluster is active and the node is healthy: `cluster show`
10. Disable disk autoassignment: `storage disk option modify -autoassign off -node node_A_2-IP`
11. If encryption is used, restore the keys using the correct command for your key management configuration.

If you are using…	Use this command…
Onboard key management	security key-manager onboard sync For more information, see Restoring onboard key management encryption keys.
External key management	security key-manager key query -node node-name For more information, see Restoring external key management encryption keys. +

12. Repeat the above steps on the second new controller module (node_B_2-IP).

Verifying MTU settings

Verify that MTU settings are set correctly for the ports and broadcast domain and make changes using the following commands

1. Check the MTU size used in the cluster broadcast domain: `network port broadcast-domain show`
2. If necessary, update the MTU size as needed: `network port broadcast-domain modify -broadcast-domain bcast-domain=name-mtu mtu-size`

Configuring intercluster LIFs

Configure the intercluster LIFs required for cluster peering.

This task must be performed on both of the new nodes, node_A_2-IP and node_B_2-IP.

1. Configure the intercluster LIFs using the procedures in the *MetroCluster IP Installation and Configuration Guide*.

   Configuring intercluster LIFs

Verifying cluster peering

Verify that cluster_A and cluster_B are peered and nodes on each cluster can communicate with each other.

1. Verify the cluster peering relationship: `cluster peer health show`

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
node_A_1-IP
           cluster_B                   node_B_1-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       node_B_2-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
node_A_2-IP
           cluster_B                   node_B_1-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       node_B_2-IP
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

2. Ping to check that the peer addresses are reachable: `cluster peer ping -originating-node local-node -destination-cluster remote-cluster-name`

Configuring the new nodes and completing transition

With the new nodes added, you must complete the transition steps and configure the MetroCluster IP nodes.

Configuring the MetroCluster IP nodes and disabling transition

You must implement the MetroCluster IP connections, refresh the MetroCluster configuration, and disable transition mode.

1. Form the new nodes into a DR group by issuing the following commands from controller node_A_1-IP `metrocluster configuration-settings dr-group create -partner-cluster peer-`

cluster-name -local-node local-controller-name -remote-node remote-controller-name``metrocluster configuration-settings dr-group show

2. Create MetroCluster IP interfaces (node_A_1-IP, node_A_2-IP, node_B_1-IP, node_B_2-IP) — two interfaces need to be created per controller; eight interfaces in total, using the following command: `metrocluster configuration-settings interface create -cluster-name cluster-name -home-node controller-name -home-port port -address ip-address -netmask netmask -vlan-id vlan-id``metrocluster configuration-settings interface show`

   > Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.

   The -vlan-id parameter is required only if you are not using the default VLAN IDs. Only certain systems support non-default VLAN IDs.

   > ◦ Starting with ONTAP 9.8, certain platforms use a VLAN for the MetroCluster IP interface. By default, each of the two ports use a different VLAN: 10 and 20. You can also specify a different (non-default) VLAN higher than 100 (between 101 and 4095) using the `-vlan-id parameter` in the `metrocluster configuration-settings interface create` command.
   >
   > ◦ Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.

   The following platform models use VLANs and allow configuration of a non-default VLAN ID.

AFF platforms	FAS platforms
• AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

3. Perform the MetroCluster connect operation from controller node_A_1-IP to connect the MetroCluster sites — this operation can take a few minutes to complete. `metrocluster configuration-settings connection connect`
4. Verify that the remote cluster disks are visible from each controller via the iSCSI connections: `disk show`

   You should see the remote disks belonging to the other nodes in the configuration.

5. Mirror the root aggregate for node_A_1-IP and node_B_1-IP: `aggregate mirror -aggregate root-aggr`
6. Assign disks for node_A_2-IP and node_B_2-IP.

   Pool 1 disk assignments where already made for node_A_1-IP and node_B_1-IP when the boot_after_mcc_transtion command was issued at the boot menu.

   a. Issue the following commands on node_A_2-IP: `disk assign disk1disk2disk3 ... diskn`

`-sysid node_B_2-IP-controller-sysid -pool 1 -force`

   b. Issue the following commands on node_B_2-IP: `disk assign disk1disk2disk3 ... diskn -sysid node_A_2-IP-controller-sysid -pool 1 -force`

7. Confirm ownership has been updated for the remote disks: `disk show`
8. If necessary, refresh the ownership information using the following commands:
   a. Go to advanced privilege mode and enter y when prompted to continue: `set priv advanced`
   b. Refresh disk ownership: `disk refresh-ownership controller-name`
   c. Return to admin mode: `set priv admin`
9. Mirror the root aggregates for node_A_2-IP and node_B_2-IP: `aggregate mirror -aggregate root-aggr`
10. Verify that the aggregate re-synchronization has completed for root and data aggregates: `aggr show``aggr plex show`

    The resync can take some time but must complete before proceeding with the following steps.

11. Refresh the MetroCluster configuration to incorporate the new nodes:
    a. Go to advanced privilege mode and enter y when prompted to continue: `set priv advanced`
    b. Refresh the configuration:

If you have configured…	Issue this command…
A single aggregate in each cluster:	`metrocluster configure -refresh true -allow-with-one-aggregate true`
More than a single aggregate in each cluster	`metrocluster configure -refresh true`

    c. Return to admin mode: `set priv admin`
12. Disable MetroCluster transition mode:
    a. Enter advanced privilege mode and enter y when prompted to continue: `set priv advanced`
    b. Disable transition mode: `metrocluster transition disable`
    c. Return to admin mode: `set priv admin`

Setting up data LIFs on the new nodes

You must configure data LIFs on the new nodes, node_A_2-IP and node_B_2-IP.

You must add any new ports available on new controllers to a broadcast domain if not already assigned to one. If required, create VLANs or interface groups on the new ports. See the *Network Management Guide*.

Network and LIF management

1. Run the following commands to identify the current port usage and broadcast domains: `network port show``network port broadcast-domain show`

2. Add ports to broadcast domains and VLANs as necessary.
   a. View the IP spaces: `network ipspace show`
   b. Create IP spaces and assign data ports as needed.

      Configuring IPspaces (cluster administrators only)

   c. View the broadcast domains: `network port broadcast-domain show`
   d. Add any data ports to a broadcast domain as needed.

      Adding or removing ports from a broadcast domain

   e. Recreate VLANs and interface groups as needed.

      VLAN and interface group membership might be different than that of the old node.

      Creating a VLAN

      Combining physical ports to create interface groups

3. Verify that the LIFs are hosted on the appropriate node and ports on the MetroCluster IP nodes (including the SVM with -mc vserver) as needed.

   See the information gathered in Creating the network configuration.

   a. Run the below command to check the home port of the LIFs: `network interface show -field home-port`
   b. If necessary, modify the LIF configuration: `vserver config override -command "network interface modify -vserver vserver_name -home-port active_port_after_upgrade -lif lif_name -home- node new_node_name"`
   c. Revert the LIFs to their home ports: `network interface revert * -vserver vserver_name`

Bringing up the SVMs

Due to the changes if LIF configuration, you must restart the SVMs on the new nodes.

1. Check the state of the SVMs: `metrocluster vserver show`
2. Restart the SVMs on cluster_A that do not have an -mc suffix: `vserver start -vserver svm-name -force true`
3. Repeat the previous steps on the partner cluster.
4. Check that all SVMs are in a healthy state: `metrocluster vserver show`
5. Verify that all data LIFs are online: `network interface show`

Moving a system volume to the new nodes

To improve resiliency, a system volume should be moved from controller node_A_1-IP to controller node_A_2-IP, and also from node_B_1-IP to node_B_2-IP. You must create a mirrored aggregate on the destination node for the system volume.

System volumes have the name form MDV_CRS_*A or MDV_CRS*B. _A and _B are unrelated to the site_A and site_B references used throughout this section; e.g., MDV_CRS*_A is not associated with site_A.

1. Assign at least three pool 0 and three pool 1 disks each for controllers node_A_2-IP and node_B_2-IP as needed.
2. Enable disk auto-assignment.
3. Move the _B system volume from node_A_1-IP to node_A_2-IP using the following steps from site_A.
   a. Create a mirrored aggregate on controller node_A_2-IP to hold the system volume: `aggr create -aggregate new_node_A_2-IP_aggr -diskcount 10 -mirror true -node nodename_node_A_2-IP``aggr show`

      The mirrored aggregate requires five pool 0 and five pool 1 spare disks owned by controller node_A_2-IP.

      The advanced option, "-force-small-aggregate true" can be used to limit disk use to 3 pool 0 and 3 pool 1 disks, if disks are in short supply.

   b. List the system volumes associated with the admin SVM: `vserver show``volume show -vserver admin-vserver-name`

      You should identify volumes contained by aggregates owned by site_A. site_B system volumes will also be shown.

4. Move the MDV_CRS_*_B system volume for site_A to the mirrored aggregate created on controller node_A_2-IP
   a. Check for possible destination aggregates: `volume move target-aggr show -vserver admin-vserver-name -volume system_vol_MDV_B`

      The newly created aggregate on node_A_2-IP should be listed.

   b. Move the volume to the newly created aggregate on node_A_2-IP: `set advanced``volume move start -vserver admin-vserver -volume system_vol_MDV_B -destination-aggregate new_node_A_2-IP_aggr -cutover-window 40`
   c. Check status for the move operation: `volume move show -vserver admin-vserver-name -volume system_vol_MDV_B`
   d. When the move operation complete, verify the MDV_CRS_*_B system is contained by the new aggregate on node_A_2-IP: `set admin``volume show -vserver admin-vserver`
5. Repeat the above steps on site_B (node_B_1-IP and node_B_2-IP).

Returning the system to normal operation

You must perform final configuration steps and return the MetroCluster configuration to normal operation.

Verifying MetroCluster operation and assigning drives after transition

You must verify that the MetroCluster is operating correctly and assign drives to the second pair of new nodes (node_A_2-IP and node_B_2-IP).

1. Confirm that the MetroCluster configuration-type is IP-fabric: `metrocluster show`
2. Perform a MetroCluster check.
   a. Issue the following command: `metrocluster check run`
   b. Display the results of the MetroCluster check: `metrocluster check show`
3. Confirm that the DR group with the MetroCluster IP nodes is configured: `metrocluster node show`
4. Create and mirror additional data aggregates for controllers node_A_2-IP and node_B_2-IP at each site as needed.

Installing licenses for the new controller module

You must add licenses for the new controller module for any ONTAP services that require standard (node-locked) licenses. For features with standard licenses, each node in the cluster must have its own key for the feature.

For detailed information about licensing, see the knowledgebase article 3013749: Data ONTAP 8.2 Licensing Overview and References on the NetApp Support Site and the *System Administration Reference*.

1. If necessary, obtain license keys for the new node on the NetApp Support Site in the My Support section under Software licenses.

   If the site does not have the license keys you need, contact your sales or support representative.

2. Issue the following command to install each license key: `system license add -license-code license_key`

   The license_key is 28 digits in length.

   Repeat this step for each required standard (node-locked) license.

Completing configuration of the nodes

There are miscellaneous configuration steps that can be performed prior to completing the procedures. Some of these steps are optional.

1. Configure the service processor: `system service-processor network modify`
2. Set up autosupport on the new nodes: `system node autosupport modify`
3. The controllers can be optionally renamed as part of the transition. The following command is used to rename a controller: `system node rename -node <old-name> -newname <new-name>`

   The renaming operation can take a few minutes to complete. Confirm that any name changes have propagated to each node prior to continuing with other steps using the system show -fields node command.

4. Configure a monitoring service as desired.

   xref:./transition/../install-ip/concept_considerations_mediator.adoc

   Configuring the ONTAP Mediator service for unplanned automatic switchover

Tiebreaker Software Installation and Configuration Guide

Sending a custom AutoSupport message after maintenance

After completing the transition, you should send an AutoSupport message indicating the end of maintenance, so automatic case creation can resume.

1. To resume automatic support case generation, send an Autosupport message to indicate that the maintenance is complete.
   a. Issue the following command: `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Repeat the command on the partner cluster.

Disruptively transitioning from MetroCluster FC to MetroCluster IP when retiring storage shelves (ONTAP 9.8 and later)

Starting with ONTAP 9.8, you can disruptively transition a two-node MetroCluster FC configuration to a four-node MetroCluster IP configuration and retire the existing storage shelves. The procedure includes steps to move data from the existing drive shelves to the new configuration, and then retire the old shelves.

- This procedure is used when you plan to retire the existing storage shelves and move all data to the new shelves in the MetroCluster IP configuration.
- The existing storage shelf models must be supported by the new MetroCluster IP nodes.
- This procedure is supported on systems running ONTAP 9.8 and later.
- This procedure is disruptive.
- This procedure applies only to a two-node MetroCluster FC configuration.

  If you have a four-node MetroCluster FC configuration, see Choosing your transition procedure.
- You must meet all requirements and follow all steps in the procedure.

Requirements for transition when retiring old shelves

Before starting the transition process, you must make sure the existing MetroCluster FC configuration meets the requirements.

- It must be a two-node fabric-attached or stretch MetroCluster configuration and all nodes must be running ONTAP 9.8 or later.

  The new MetroCluster IP controller modules should be running the same version of ONTAP 9.8.
- The existing and new platforms must be a supported combination for transition.

  Supported platforms for nondisruptive transition
- It must meet all requirements and cabling as described in the *MetroCluster Installation and Configuration*

Guides.

Fabric-attached MetroCluster installation and configuration

The new configuration must also meet the following requirements:

- The new MetroCluster IP platform models must support the old storage shelf models.

  NetApp Hardware Universe

- Depending on the spare disks available in the existing shelves, additional drives must be added.

  This might require additional drive shelves.

  You need to have additional 14 - 18 drives for each controller:

  - Three pool 0 drives
  - Three pool 1 drives
  - Two spare drives
  - Six to ten drives for the system volume

- You must ensure that the configuration, including the new nodes, does not exceed the platform limits for the configuration, including drive count, root aggregate size capacity, etc.

  This information is available for each platform model at *NetApp Hardware Universe*.

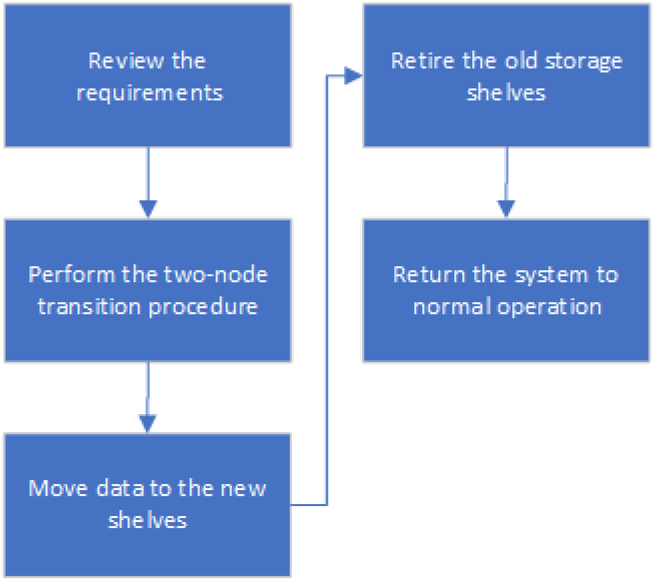
  NetApp Hardware Universe

You must have remote console access for all six nodes from either MetroCluster site or plan for travel between the sites as required by the procedure.

Workflow for disruptive transition when moving data and retiring old storage shelves

You must follow the specific workflow to ensure a successful transition.

As you prepare for the transition, plan for travel between the sites. Note that after the remote nodes are racked and cabled, you need serial terminal access to the nodes. Service Processor access is not be available until the nodes are configured.



Transitioning the configuration

You must follow the detailed transition procedure.

In the following steps you are directed to other sections in this guide. You must perform the steps in each referenced section in the order given.

1. Plan port mapping using the steps in Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes.
2. Prepare the MetroCluster IP controllers using the steps in Preparing the MetroCluster IP controllers.
3. Verify the health of the MetroCluster FC configuration.

   Perform the steps in the section Verifying the health of the MetroCluster FC configuration

4. Gather information from the MetroCluster FC configuration.

   Perform the steps in the section Gathering information from the existing controller modules before the transition

5. Remove Tiebreaker monitoring, if necessary.

   Perform the steps in the section Removing the existing configuration from the Tiebreaker or other monitoring software

6. Prepare and remove the existing MetroCluster FC nodes.

   Perform the steps in the section Transitioning the MetroCluster FC nodes.

7. Connect the new MetroCluster IP nodes.

   Perform the steps in the section Connecting the MetroCluster IP controller modules.

8. Configure the new MetroCluster IP nodes and complete transition.

   Perform the steps in the section Configuring the new nodes and completing transition.

Migrating the root aggregates

After the transition is complete, migrate the existing root aggregates leftover from the MetroCluster FC configuration to new shelves in the MetroCluster IP configuration.

This task moves the root aggregates for node_A_1-FC and node_B_1-FC to disk shelves owned by the new MetroCluster IP controllers:

1. Assign pool 0 disks on the new local storage shelf to the controller that has the root being migrated (e.g., if the root of node_A_1-FC is being migrated, assign pool 0 disks on the new shelf to node_A_1-IP)

   Note that the migration *removes and does not re-create the root mirror*, so pool 1 disks do not need to be assigned before issuing the migrate command

2. Set the privilege mode to advanced: `set priv advanced`
3. Migrate the root aggregate: `system node migrate-root -node node-name -disklist disk-id1,disk-id2,diskn -raid-type raid-type`
   - The node-name is the node to which the root aggregate is being migrated.
   - The disk-id identifies the pool 0 disks on the new shelf.
   - The raid-type is normally the same as the raid-type of the existing root aggregate.
   - You can use the command job show -idjob-id-instance to check the migration status, where job-id is the value provided when the migrate-root command is issued. For example, if the root aggregate for node_A_1-FC consisted of three disks with raid_dp, the following command would be used to migrate root to a new shelf 11:

   ```
   system node migrate-root -node node_A_1-IP -disklist
   3.11.0,3.11.1,3.11.2 -raid-type raid_dp
   ```

4. Wait until the migration operation completes and the node automatically reboots.
5. Assign pool 1 disks for the root aggregate on a new shelf directly connected to the remote cluster.
6. Mirror the migrated root aggregate.
7. Wait for the root aggregate to complete resynchronising.

   You can use the storage aggregate show command to check the sync status of the aggregates.

8. Repeat these steps for the other root aggregate.

Migrating the data aggregates

Create data aggregates on the new shelves and use volume move to transfer the data volumes from the old shelves to the aggregates on the new shelves.

1. Move the data volumes to aggregates on the new controllers, one volume at a time.

   Use the following section of the *Controller Upgrade Express Guide*.

   Creating an aggregate and moving volumes to the new nodes

Retiring shelves moved from node_A_1-FC and node_A_2-FC

You retire the old storage shelves from the original MetroCluster FC configuration. These shelves were originally owned by node_A_1-FC and node_A_2-FC.

1. Identify the aggregates on the old shelves on cluster_B that need to be deleted.

   In this example the following data aggregates are hosted by the MetroCluster FC cluster_B and need to be deleted: aggr_data_a1 and aggr_data_a2.

   > You need to perform the steps to identify, offline and delete the data aggregates on the shelves. The example is for one cluster only.

   ```
   cluster_B::> aggr show

   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   aggr0_node_A_1-FC
              349.0GB   16.83GB   95% online       1 node_A_1-IP
   raid_dp,

   mirrored,

   normal
   aggr0_node_A_2-IP
              349.0GB   16.83GB   95% online       1 node_A_2-IP
   raid_dp,

   mirrored,

   normal
   ...
   8 entries were displayed.

   cluster_B::>
   ```

2. Check if the data aggregates have any MDV_aud volumes, and delete them prior to deleting the aggregates.

   You must delete the MDV_aud volumes as they cannot be moved.

3. Take each of the aggregates offline, and then delete them:

   a. Take the aggregate offline: `storage aggregate offline -aggregate aggregate-name`

      The following example shows the aggregate node_B_1_aggr0 being taken offline:

```
cluster_B::> storage aggregate offline -aggregate node_B_1_aggr0

Aggregate offline successful on aggregate: node_B_1_aggr0
```

b. Delete the aggregate: `storage aggregate delete -aggregate aggregate-name`

You can destroy the plex when prompted.

The following example shows the aggregate node_B_1_aggr0 being deleted.

```
cluster_B::> storage aggregate delete -aggregate node_B_1_aggr0
Warning: Are you sure you want to destroy aggregate "node_B_1_aggr0"?
{y|n}: y
[Job 123] Job succeeded: DONE

cluster_B::>
```

4. After deleting all aggregates, power down, disconnect, and remove the shelves.
5. Repeat the above steps to retire the cluster_A shelves.

Completing transition

With the old controller modules removed, you can complete the transition process.

1. Complete the transition process.

   Perform the steps in Returning the system to normal operation

Disruptively transitioning when existing shelves are not supported on new controllers (ONTAP 9.8 and later)

Starting with ONTAP 9.8, you can disruptively transition a two-node MetroCluster FC configuration and move data from the existing drive shelves even if the existing storage shelves are not supported by the new MetroCluster IP nodes.

- This procedure should only be used if the existing storage shelf models are not supported by the new MetroCluster IP platform models.
- This procedure is supported on systems running ONTAP 9.8 and later.
- This procedure is disruptive.
- This procedure applies only to a two-node MetroCluster FC configuration.

  If you have a four-node MetroCluster FC configuration, see Choosing your transition procedure.

- You must meet all requirements and follow all steps in the procedure.

Requirements for transition when shelves are not supported on the new nodes

Before starting the transition process, you must make sure the configuration meets the requirements.

- The existing configuration must be a two-node fabric-attached or stretch MetroCluster configuration and all nodes must be running ONTAP 9.8 or later.

  The new MetroCluster IP controller modules should be running the same version of ONTAP 9.8.

- The existing and new platforms must be a supported combination for transition.

  Supported platforms for nondisruptive transition

- It must meet all requirements and cabling as described in the *MetroCluster Installation and Configuration Guides*.

  Fabric-attached MetroCluster installation and configuration

- New storage shelves provided with the new controllers (node_A_1-IP, node_A_2-IP, node_B_1-IP and node_B_2-IP) must be supported by the old controllers (node_A_1-FC and node_B_1-FC).

  NetApp Hardware Universe

- The old storage shelves are **not** supported by the new MetroCluster IP platform models.

  NetApp Hardware Universe

- Depending on the spare disks available in the existing shelves, additional drives must be added.

  This might require additional drive shelves.

  You need to have additional 14 to 18 drives for each controller:

  - Three pool0 drives
  - Three pool1 drives
  - Two spare drives
  - Six to ten drives for the system volume

- You must ensure that the configuration, including the new nodes, does not exceed the platform limits for the configuration, including drive count, root aggregate size capacity, etc.

  This information is available for each platform model at *NetApp Hardware Universe*.

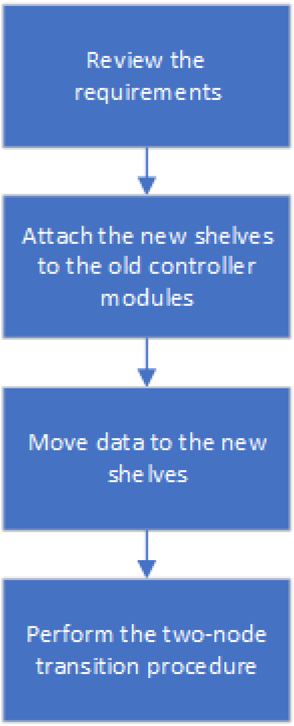
  NetApp Hardware Universe

- You must have remote console access for all six nodes from either MetroCluster site or plan for travel between the sites as required by the procedure.

Workflow for disruptive transition when shelves are not supported by new controllers

If the existing shelf models are not supported by the new platform models, you must attach the new shelves to the old configuration, move data onto the new shelves, and then transition to the new configuration.

As you prepare for the transition, plan for travel between the sites. Note that after the remote nodes are racked and cabled, you need serial terminal access to the nodes. Service Processor access is not be available until the nodes are configured.



Preparing the new controller modules

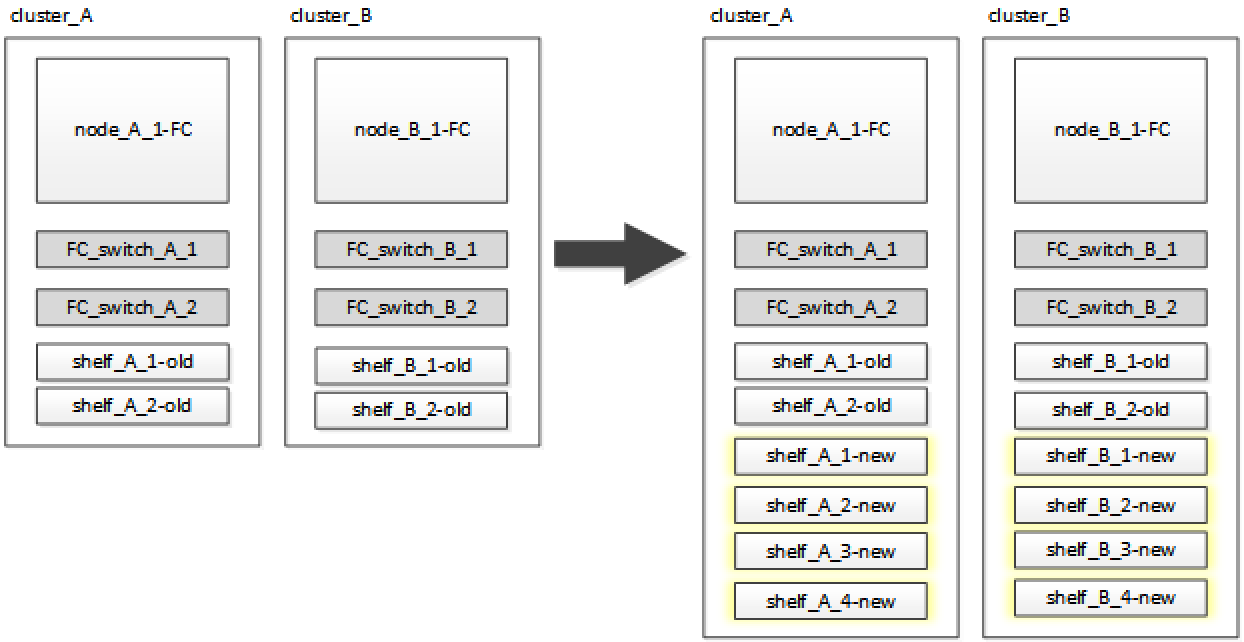
You must clear the configuration and disk ownership on the new controller modules and the new storage shelves.

1. With the new storage shelves attached to the new MetroCluster IP controller modules, perform all the steps in the secontion Preparing the MetroCluster IP controllers.
2. Disconnect the new storage shelves from the new MetroCluster IP controller modules.

Attaching the new disk shelves to the existing MetroCluster FC controllers

You must attach the new drive shelves to the existing controller modules before transitioning to a MetroCluster IP configuration.

The following illustration shows the new shelves attached to the MetroCluster FC configuration.



1. Disable disk autoassignment on node_A_1-FC and node_A_2-FC: `disk option modify -node node-name -autoassign off`

   This command must be issued on each node.

   Disk auto-assign is disabled to avoid assignment of the shelves to be added to node_A_1-FC and node_B_1-FC. As part the transition, disks are needed for nodes node_A_1-IP and node_B_2-IP and if autoassign is allowed, disk ownership would later need to be removed before disks could be assigned to node_A_1-IP and node_B_2-IP.

2. Attach the new shelves to the existing MetroCluster FC nodes, using FC-to-SAS bridges, if necessary.

   See the requirements and procedures in the described in the *MetroCluster Maintenance Guide*.

   Hot-adding storage to a MetroCluster FC configuration

Migrate root aggregates and move data to the new disk shelves

You must move the root aggregates from the old drive shelves to the new drive shelves that will be used by the MetroCluster IP nodes.

This task is performed prior to the transition on the existing nodes (node_A_1-FC and node_B_1-FC).

1. Perform a negotiated switchover from controller node_B_1-FC: `metrocluster switchover`
2. Perform the heal aggregates and heal root steps of the recovery from node_B_1-FC: `metrocluster heal -phase aggregates``metrocluster heal -phase root-aggregates`
3. Boot controller node_A_1-FC: `boot_ontap`
4. Assign the unowned disks on the new shelves to the appropriate pools for controller node_A_1-FC:
   a. Identify the disks on the shelves: `disk show -shelf pool_0_shelf -fields container-type,diskpathnames``disk show -shelf pool_1_shelf -fields container-type,diskpathnames`

b. Enter local mode so the commands are run on the local node: `run local`

c. Assign the disks: `disk assign disk1disk2disk3disk… -p 0``disk assign disk4disk5disk6disk… -p 1`

d. Exit local mode: `exit`

5. Create a new mirrored aggregate to become the new root aggregate for controller node_A_1-FC:

   a. Set the privilege mode to advanced: `set priv advanced`

   b. Create the aggregate: `aggregate create -aggregate new_aggr -disklist disk1, disk2, disk3,… -mirror-disklist disk4disk5, disk6,… -raidtypesame-as -existing-root -force-small-aggregate true aggr show -aggregate new_aggr -fields percent-snapshot-space`

      If the percent-snapshot-space value is less than 5 percent, you must increase it to a value higher than 5 percent: `aggr modify new_aggr -percent-snapshot-space 5`

   c. Set the privilege mode back to admin: `set priv admin`

6. Confirm that the new aggregate is created properly: `node run -node local sysconfig -r`

7. Create the node and cluster-level configuration backups:

   > When the backups are created during switchover, the cluster is aware of the switched over state on recovery. You must ensure that the backup and upload of the system configuration is successful as without this backup it is **not** possible to reform the MetroCluster configuration between clusters.

   a. Create the cluster backup: `system configuration backup create -node local -backup -type cluster -backup-name cluster-backup-name`

   b. Check cluster backup creation `job show -id job-idstatus`

   c. Create the node backup: `system configuration backup create -node local -backup -type node -backup-name node-backup-name`

   d. Check for both cluster and node backups: `system configuration backup show`

      You can repeat the command until both backups are shown in the output.

8. Make copies of the backups.

   The backups must be stored at a separate location because they will be lost locally when the new root volume is booted.

   You can upload the backups to an FTP or HTTP server, or copy the backups using scp commands.

Method	
Upload the backup to the FTP or HTTP server	a. Upload the cluster backup: `system configuration backup upload -node local -backup cluster-backup-name -destination URL` b. Upload the node backup: `system configuration backup upload -node local -backup node-backup-name -destination URL`
Copy the backups onto a remote server using secure copy	`From the remote server use the following scp commands:` a. Copy the cluster backup: `scp diagnode-mgmt-FC:/mroot/etc/backups/config/cluster-backup-name.7z .` b. Copy the node backup: `scp diag@node-mgmt-FC:/mroot/etc/backups/config/node-backup-name.7z .`

9. Halt node_A_1-FC: `halt -node local -ignore-quorum-warnings true`
10. Boot node_A_1-FC to Maintenance mode: `boot_ontap maint`
11. From Maintenance mode, make required changes to set the aggregate as root:
    a. Set the HA policy to cfo: `aggr options new_aggr ha_policy cfo`

       Respond `yes` when prompted to proceed.

       ```
       Are you sure you want to proceed (y/n)?
       ```

    b. Set the new aggregate as root: `aggr options new_aggr root`
    c. Halt to the LOADER prompt: `halt`
12. Boot the controller and back up the system configuration.

    The node boots in recovery mode when the new root volume is detected

    a. Boot the controller: `boot_ontap`
    b. Log in and back up the configuration.

       When you log in, you will see the following warning:

```
Warning: The correct cluster system configuration backup must be
restored. If a backup
from another cluster or another system state is used then the root
volume will need to be
recreated and NGS engaged for recovery assistance.
```

c. Enter advanced privilege mode: `set -privilege advanced`
d. Back up the cluster configuration to a server: `system configuration backup download -node local -source URL of server/cluster-backup-name.7z`
e. Back up the node configuration to a server: `system configuration backup download -node local -source URL of server/node-backup-name.7z`
f. Return to admin mode: `set -privilege admin`

13. Check the health of the cluster:
    a. Issue the following command: `cluster show`
    b. Set the privilege mode to advanced: `set -privilege advanced`
    c. Verify the cluster configuration details: `cluster ring show`
    d. Return to the admin privilege level: `set -privilege admin`
14. Confirm the operational mode of the MetroCluster configuration and perform a MetroCluster check.
    a. Confirm the MetroCluster configuration and that the operational mode is normal: `metrocluster show`
    b. Confirm that all expected nodes are shown: `metrocluster node show`
    c. Issue the following command: `metrocluster check run`
    d. Display the results of the MetroCluster check: `metrocluster check show`
15. Perform a switchback from controller node_B_1-FC: `metrocluster switchback`
16. Verify the operation of the MetroCluster configuration:
    a. Confirm the MetroCluster configuration and that the operational mode is normal: `metrocluster show`
    b. Perform a MetroCluster check: `metrocluster check run`
    c. Display the results of the MetroCluster check: `metrocluster check show`
17. Add the new root volume to the Volume Location Database.
    a. Set the privilege mode to advanced: `set -privilege advanced`
    b. Add the volume to the node: `volume add-other-volumes –node node_A_1-FC`
    c. Return to the admin privilege level: `set -privilege admin`
18. Check that the volume is now visible and has mroot.
    a. Display the aggregates: `storage aggregate show`
    b. Verify that the root volume has mroot: `storage aggregate show -fields has-mroot`

c. Display the volumes: `volume show`

19. Create a new security certificate to re-enable access to System Manager: `security certificate create -common-name name -type server -size 2048`
20. Repeat the previous steps to migrate the aggregates on shelves owned by node_A_1-FC.
21. Perform a cleanup.

    You must perform the following steps on both node_A_1-FC and node_B_1-FC to remove the old root volume and root aggregate.

    a. Delete the old root volume: `run localvol offline old_vol0vol destroy old_vol0 exitvolume remove-other-volume -vserver node_name -volume old_vol0`

    b. Delete the original root aggregate: `aggr offline -aggregate old_aggr0_site``aggr delete -aggregate old_aggr0_site`
22. Migrate the data volumes to aggregates on the new controllers, one volume at a time.

    Use the following section of the *Controller Upgrade Express Guide*.

    Creating an aggregate and moving volumes to the new nodes
23. Retire the old shelves by performing all the steps in the section Retiring shelves moved from node_A_1-FC and node_A_2-FC.

Transitioning the configuration

You must follow the detailed transition procedure.

In the following steps you are directed to other sections in this guide. You must perform the steps in each referenced section in the order given.

1. Plan port mapping.

   Perform all the steps in the section Mapping ports from the MetroCluster FC nodes to the MetroCluster IP nodes.
2. Prepare the MetroCluster IP controllers.

   Perform all the steps in the section Preparing the MetroCluster IP controllers.
3. Verify the health of the MetroCluster configuration.

   Perform all the steps in the section Verifying the health of the MetroCluster FC configuration
4. Prepare and remove the existing MetroCluster FC nodes.

   Perform all the steps in the section Transitioning the MetroCluster FC nodes.
5. Add the new MetroCluster IP nodes.

   Perform all the steps in the section Connecting the MetroCluster IP controller modules.
6. Complete the transition and initial configuration of the new MetroCluster IP nodes.

Perform all the steps in the section Configuring the new nodes and completing transition.

Moving an FC SAN workload from MetroCluster FC to MetroCluster IP nodes

When non-disruptively transitioning from MetroCluster FC to IP nodes, you must non-disruptively move FC SAN host objects from MetroCluster FC to IP nodes.

1. Set up new FC interfaces (LIFS) on MetroCluster IP nodes:
   a. If required, on MetroCluster IP nodes, modify FC ports to be used for client connectivity to FC target personality.

      This may require a reboot of the nodes.
   b. Create FC LIFS/interfaces on IP nodes for all SAN vservers. Optionally verify that the WWPNs from newly created FC LIFs are logged into the FC SAN switch
2. Update SAN zoning configuration for newly added FC LIFs on MetroCluster IP nodes.

   To facilitate moving of volumes that contain LUNs actively serving data to FC SAN clients, update existing FC switch zones to allow FC SAN clients to access to LUNs on MetroCluster IP nodes.
   a. On the FC SAN switch (Cisco or Brocade), add the WWPNs of newly added FC SAN LIFs to the zone.
   b. Update, save and commit the zoning changes.
   c. From the client, check for FC initiator logins to the new SAN LIFs on the MetroCluster IP nodes: `sanlun lun show -p`

      At this time, the client should see and be logged in to the FC interfaces on both the MetroCluster FC and MetroCluster IP nodes. LUNs and volumes are still physically hosted on the MetroCluster FC nodes.

      Because LUNs are reported only on MetroCluster FC node interfaces, the client shows only paths over FC nodes. This can be seen in the output of the sanlun lun show -p and multipath -ll -d commands.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_

[root@stemgr]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

3. Modify the reporting nodes to add the MetroCluster IP nodes
   a. List reporting nodes for LUNs on the SVM: `lun mapping show -vserver svm-name -fields reporting-nodes -ostype linux`

      Reporting nodes shown are local nodes as LUNs are physically on FC nodes A_1 and A_2.

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver  path                         igroup        reporting-nodes
-------  ---------------------------- ------------
-------------------------------------
vsa_1    /vol/vsa_1_vol1/lun_linux_2 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol1/lun_linux_3 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol2/lun_linux_4 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol3/lun_linux_7 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_8 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol4/lun_linux_9 igroup_linux   A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_12 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol6/lun_linux_13 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol7/lun_linux_14 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol8/lun_linux_17 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_18 igroup_linux  A_1,A_2
vsa_1    /vol/vsa_1_vol9/lun_linux_19 igroup_linux  A_1,A_2
12 entries were displayed.
```

b. Add reporting nodes to include MetroCluster IP nodes.

```
cluster_A::> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes B_1,B_2 -igroup igroup_linux

12 entries were acted on.
```

c. List reporting nodes and verify the presence of the new nodes:

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path                          igroup          reporting-nodes
------- ---------------------------   ------------
------------------------------------------------------------------------
----------

vsa_1   /vol/vsa_1_vol1/lun_linux_2   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol1/lun_linux_3   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol2/lun_linux_4   igroup_linux    A_1,A_2,B_1,B_2
vsa_1   /vol/vsa_1_vol3/lun_linux_7   igroup_linux    A_1,A_2,B_1,B_2
...

12 entries were displayed.
```

d. Rescan the scsi bus on the host to discover the newly added paths: `/usr/bin/rescan-scsi-bus.sh -a`

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

e. Display the newly added paths: `sanlun lun show -p`

Each LUN will have four paths.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_
up secondary sdag host4 iscsi_lf__n4_p1_
up secondary sdah host5 iscsi_lf__n3_p1_
```

f. On the controllers, move the volumes containing LUNs from the MetroCluster FC to the MetroCluster IP nodes.

```
cluster_A::> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate A_1_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "A_1_htp_005_aggr1". Use the "volume move show -vserver
vsa_1 -volume vsa_1_vol1"
command to view the status of this operation.
cluster_A::> volume move show
Vserver    Volume    State    Move Phase   Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------   ----------------
----------------
vsa_1     vsa_1_vol1 healthy  initializing
 - -
```

g. On the FC SAN client, display the LUN information: `sanlun lun show -p`

The FC interfaces on the MetroCluster IP nodes where the LUN now resides are updated as primary paths. If the primary path is not updated after the volume move, run /usr/bin/rescan-scsi-bus.sh -a or simply wait for multipath rescanning to take place.

The primary path in the following example is the LIF on MetroCluster IP node.

```
[root@localhost ~]# sanlun lun show -p

                    ONTAP Path: vsa_1:/vol/vsa_1_vol1/lun_linux_2
                           LUN: 22
                      LUN Size: 2g
                       Product: cDOT
                   Host Device: 3600a098038302d324e5d50305063546e
              Multipath Policy: service-time 0
            Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host      vserver
path      path       /dev/   host         vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------
----------------------------------------------
up        primary    sddv    host6        fc_5
up        primary    sdjx    host7        fc_6
up        secondary  sdgv    host6        fc_8
up        secondary  sdkr    host7        fc_8
```

h. Repeat the above steps for all volumes, LUNs and FC interfaces belonging to a FC SAN host.

   When completed, all LUNs for a given SVM and FC SAN host should be on MetroCluster IP nodes.

4. Remove the reporting nodes and re-scan paths from client.

   a. Remove the remote reporting nodes (the MetroCluster FC nodes) for the linux LUNs: `lun mapping remove-reporting-nodes -vserver vsa_1 -path * -igroup igroup_linux -remote -nodes true`

```
cluster_A::> lun mapping remove-reporting-nodes -vserver vsa_1 -path
* -igroup igroup_linux -remote-nodes true
12 entries were acted on.
```

   b. Check reporting nodes for the LUNs: `lun mapping show -vserver vsa_1 -fields reporting-nodes -ostype linux`

```
cluster_A::> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path igroup reporting-nodes
------- --------------------------- ------------
----------------------------------------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux B_1,B_2
vsa_1 /vol/vsa_1_vol2/lun_linux_4 igroup_linux B_1,B_2
...

12 entries were displayed.
```

c. Rescan the scsi bus on the client: `/usr/bin/rescan-scsi-bus.sh -r`

The paths from the MetroCluster FC nodes are removed:

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
...
```

d. Verify that only paths from the MetroCluster IP nodes are visible from the host: `sanlun lun show -p`

e. If required, remove iSCSI LIFs from the MetroCluster FC nodes.

   This should be done if there are no other LUNs on the nodes mapped to other clients.

Moving Linux iSCSI hosts from MetroCluster FC to MetroCluster IP nodes

After you transition your MetroCluster nodes from FC to IP, you might need to move your iSCSI host connections to the new nodes.

In this procedure IPv4 interfaces are created.

The host commands and examples given in these procedures are specific to LINUX operating systems.

Setting up new iSCSI connections

To move iSCSI connections, you must set up new iSCSI connections to the MetroCluster IP nodes.

1. Create iSCSI interfaces on the MetroCluster IP nodes and check ping connectivity from the iSCSI clients to the new IP interfaces on the MetroCluster IP nodes.

   Creating network interfaces

   All iSCSI interfaces from the SVM should be reachable by iSCSI client.

2. On the iSCSI host or client, identify the existing iSCSI connections from the host to the MetroCluster FC node: `iscsiadm -m session`

```
[root@scspr1789621001 ~]# iscsiadm -m session

tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)

tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
```

3. Verify the connections from the MetroCluster IP node: `iscsi session show -vserver svm-name`

```
node_A_1-IP::*> iscsi session show -vserver vsa_1

 Tpgroup Initiator Initiator

Vserver Name TSIH Name ISID Alias
--------- ------- ---- ------------------------ ---------
---------------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01
scspr1789621001.gdl.englab.netapp.com
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02
scspr1789621001.gdl.englab.netapp.com

2 entries were displayed.
```

4. List the iscsi interfaces in ONTAP for the SVM that contains the interfaces: `iscsi interface show -vserver svm-name`

```
sti8200mcchtp001htp_siteA::*> iscsi interface show -vserver vsa_1

 Logical Status Curr Curr

Vserver    Interface  TPGT Admin/Oper IP Address Node Port Enabled
---------- ---------- ---- ---------- --------------- ----------- ----
-------

vsa_1 iscsi_lf__n1_p1_ 1156 up/up 10.230.68.236 sti8200mcc-htp-001 e0g
true
vsa_1 iscsi_lf__n1_p2_ 1157 up/up fd20:8b1e:b255:805e::78c9 sti8200mcc-
htp-001 e0h true
vsa_1 iscsi_lf__n2_p1_ 1158 up/up 10.230.68.237 sti8200mcc-htp-002 e0g
true
vsa_1 iscsi_lf__n2_p2_ 1159 up/up fd20:8b1e:b255:805e::78ca sti8200mcc-
htp-002 e0h true
vsa_1 iscsi_lf__n3_p1_ 1183 up/up 10.226.43.134 sti8200mccip-htp-005 e0c
true
vsa_1 iscsi_lf__n4_p1_ 1188 up/up 10.226.43.142 sti8200mccip-htp-006 e0c
true

6 entries were displayed.
```

5. On the iSCSI client, run discovery on any one of the iSCSI IP addresses on the SVM to discover the new targets: `iscsiadm -m discovery -t sendtargets -p iscsi-ip-address`

Discovery can be run on any IP address of the SVM, including non-iSCSI interfaces.

```
[root@scspr1789621001 ~]# iscsiadm -m discovery -t sendtargets -p
10.230.68.236:3260

10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.226.43.134:3260,1183 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6
```

6. On the iSCSI client, login to all the discovered addresses: `iscsiadm -m node -L all -T node-address -p portal-address -l`

```
[root@scspr1789621001 ~]# iscsiadm -m node -L all -T iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 -p
10.230.68.236:3260 -l

Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] (multiple)
Logging in to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] (multiple)
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.142,3260] successful.
Login to [iface: default, target: iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6, portal:
10.226.43.134,3260] successful.
```

7. On the iSCSI client, verify the login and connections: `iscsiadm -m session`

```
[root@scspr1789621001 ~]# iscsiadm -m session

tcp: [1] 10.230.68.236:3260,1156 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [2] 10.230.68.237:3260,1158 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
tcp: [3] 10.226.43.142:3260,1188 iqn.1992-
08.com.netapp:sn.58d7f6df2cc611eaa9c500a098a71638:vs.6 (non-flash)
```

8. From the MetroCluster node, verify the login and connection with the client: `iscsi initiator show -vserver vsa_1`

```
sti8200mcchtp001htp_siteA::*> iscsi initiator show -vserver vsa_1

 Tpgroup Initiator

Vserver Name             TSIH Name                     ISID
Igroup Name
------- --------         ---- --------------------- -----------------
-----------------
vsa_1 iscsi_lf__n1_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:01 igroup_linux
vsa_1 iscsi_lf__n2_p1_ 4 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:02 igroup_linux
vsa_1 iscsi_lf__n3_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:04 igroup_linux
vsa_1 iscsi_lf__n4_p1_ 1 iqn.2020-
01.com.netapp.englab.gdl:scspr1789621001 00:02:3d:00:00:03 igroup_linux

4 entries were displayed.
```

At the end of this tasks, the client can see all iSCSI interfaces (on the MetroCluster FC and MetroCluster IP nodes) and is logged in to all those interfaces.

LUNs and volumes are still physically hosted on FC nodes. Because LUNs are reported only on MetroCluster FC node interfaces, the client will show only paths over MetroCluster FC nodes. This can be seen in sanlun lun show -p and multipath -ll -d command outputs. The next step is to add IP nodes as reporting nodes.

```
[root@scspr1789621001 ~]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state     type       node     adapter     LIF
--------- ---------- ------- ------------
----------------------------------------------
up        primary    sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_

[root@scspr1789621001 ~]# multipath -ll -d
3600a098038304646513f4f674e52774b dm-5 NETAPP ,LUN C-Mode
size=2.0G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 3:0:0:4 sdk 8:160 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
 `- 2:0:0:4 sdh 8:112 active ready running
```

Adding the MetroCluster IP nodes as reporting nodes

After setting up the connections to the new MetroCluster IP nodes, you must add new reporting nodes.

1. On the MetroCluster node, list reporting nodes for LUNs on the SVM: `lun mapping show -vserver vsa_1 -fields reporting-nodes -ostype linux`

   The following reporting nodes are local nodes as LUNs are physically on FC nodes node_A_1-FC and node_A_2-FC.

```
node_A_1-IP::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver path igroup reporting-nodes
-------- --------------------------- ------------
-------------------------------------
vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux node_A_1-FC,node_A_2-FC
.
.
.
vsa_1 /vol/vsa_1_vol9/lun_linux_19 igroup_linux node_A_1-FC,node_A_2-FC
12 entries were displayed.
```

2. On the MetroCluster node, add reporting nodes: `lun mapping add-reporting-nodes -vserver svm-name -path /vol/vsa_1_vol*/lun_linux_* -nodes node1,node2 -igroup igroup_linux`

```
node_A_1-IP::*> lun mapping add-reporting-nodes -vserver vsa_1 -path
/vol/vsa_1_vol*/lun_linux_* -nodes node_A_1-IP,node_A_2-IP
-igroup igroup_linux

12 entries were acted on.
```

3. On the MetroCluster node, verify that the newly added nodes are present: `lun mapping show -vserver svm-name -fields reporting-nodes -ostype linux vserver path igroup reporting-nodes`

```
node_A_1-IP::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux vserver path igroup reporting-nodes
-------- --------------------------- ------------
--------------------------------------------------------------------------
-------

vsa_1 /vol/vsa_1_vol1/lun_linux_2 igroup_linux node_A_1-FC,node_A_2-
FC,node_A_1-IP,node_A_2-IP
vsa_1 /vol/vsa_1_vol1/lun_linux_3 igroup_linux node_A_1-FC,node_A_2-
FC,node_A_1-IP,node_A_2-IP.
.
.
.

12 entries were displayed.
```

4. On the host, issue the following command to rescan the scsi bus on the host and discover the newly added paths:`/usr/bin/rescan-scsi-bus.sh -a`

```
[root@stemgr]# /usr/bin/rescan-scsi-bus.sh -a
Scanning SCSI subsystem for new devices
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
 Scanning for device 2 0 0 0 ...
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
0 device(s) removed.
```

5. On the host, issue the following command to list the newly added paths: `sanlun lun show -p`

   Four paths are shown for each LUN.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------
----------------------------------------------
host vserver
path path /dev/ host vserver
state type node adapter LIF
--------- ---------- ------- ------------
----------------------------------------------
up primary sdk host3 iscsi_lf__n2_p1_
up secondary sdh host2 iscsi_lf__n1_p1_
up secondary sdag host4 iscsi_lf__n4_p1_
up secondary sdah host5 iscsi_lf__n3_p1_
```

6. On the MetroCluster, move the volume/volumes containing LUNs from FC to IP nodes.

```
node_A_1-IP::*> vol move start -vserver vsa_1 -volume vsa_1_vol1
-destination-aggregate sti8200mccip_htp_005_aggr1
[Job 1877] Job is queued: Move "vsa_1_vol1" in Vserver "vsa_1" to
aggregate "sti8200mccip_htp_005_aggr1". Use the "volume move show
-vserver
vsa_1 -volume vsa_1_vol1" command to view the status of this operation.
node_A_1-IP::*> vol move show
Vserver    Volume     State       Move       Phase            Percent-
Complete  Time-To-Complete
---------  ---------- --------    ---------- ----------------
----------------  ----------------
vsa_1     vsa_1_vol1  healthy                initializing     -
-
```

7. When the volume move is completed, on the MetroCluster, use the volume show command to confirm that the volume or LUN is online.
8. The iSCSI interfaces on the MetroCluster IP nodes where the LUN now resides are updated as primary paths. If the primary path is not updated after the volume move, run /usr/bin/rescan-scsi-bus.sh -a and multipath -v3 or simply wait for multipath rescanning to take place.

   In the following example, the primary path is a LIF on the MetroCluster IP node.

```
[root@stemgr]# sanlun lun show -p
ONTAP Path: vsa_1:/vol/vsa_1_vol6/lun_linux_12
 LUN: 4
 LUN Size: 2g
 Product: cDOT
 Host Device: 3600a098038304646513f4f674e52774b
 Multipath Policy: service-time 0
 Multipath Provider: Native
--------- ---------- ------- ------------ ----------------------
host vserver
path path /dev/ host vserver
state     type       node    adapter      LIF
--------- ---------- ------- ------------ ------------------------
up        primary    sdag    host4        iscsi_lf__n4_p1_
up        secondary  sdk     host3        iscsi_lf__n2_p1_
up        secondary  sdh     host2        iscsi_lf__n1_p1_
up        secondary  sdah    host5        iscsi_lf__n3_p1_
```

Removing reporting nodes and rescanning paths

You must remove the reporting nodes and rescan the paths.

1. From the MetroCluster IP node, remove remote reporting nodes (the MetroCluster IP nodes) for the Linux LUNs: `lun mapping remove-reporting-nodes -vserver vsa_1 -path * -igroup igroup_linux -remote-nodes true`

   In this case, the remote nodes are FC nodes.

```
node_A_1-IP::*> lun mapping remove-reporting-nodes -vserver vsa_1 -path
* -igroup igroup_linux -remote-nodes true

12 entries were acted on.
```

2. From the MetroCluster IP node, check reporting nodes for the LUNs: `lun mapping show -vserver vsa_1 -fields reporting-nodes -ostype linux`

```
node_A_1-IP::*> lun mapping show -vserver vsa_1 -fields reporting-nodes
-ostype linux

vserver  path                        igroup      reporting-nodes
------- --------------------------- ------------
-----------------------------------------

vsa_1 /vol/vsa_1_vol1/lun_linux_2   igroup_linux  node_A_1-IP,node_A_2-
IP
vsa_1 /vol/vsa_1_vol1/lun_linux_3   igroup_linux  node_A_1-IP,node_A_2-
IP
vsa_1 /vol/vsa_1_vol2/lun_linux_4   group_linux   node_A_1-IP,node_A_2-
IP
.
.
.

12 entries were displayed.
```

3. On the iSCSI host, rescan the scsi bus: `/usr/bin/rescan-scsi-bus.sh -r`

   The paths that are removed are the paths from FC nodes.

```
[root@scspr1789621001 ~]# /usr/bin/rescan-scsi-bus.sh -r
Syncing file systems
Scanning SCSI subsystem for new devices and remove devices that have
disappeared
Scanning host 0 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 1 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
Scanning host 2 for SCSI target IDs 0 1 2 3 4 5 6 7, all LUNs
sg0 changed: LU not available (PQual 1)
REM: Host: scsi2 Channel: 00 Id: 00 Lun: 00
DEL: Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
sg2 changed: LU not available (PQual 1)
.
.
.
OLD: Host: scsi5 Channel: 00 Id: 00 Lun: 09
 Vendor: NETAPP Model: LUN C-Mode Rev: 9800
 Type: Direct-Access ANSI SCSI revision: 05
0 new or changed device(s) found.
0 remapped or resized device(s) found.
24 device(s) removed.
 [2:0:0:0]
 [2:0:0:1]
 .
.
.
```

4. On the iSCSI host, verify that only paths from the MetroCluster IP nodes are visible: `sanlun lun show -p``multipath -ll -d`

Where to find additional information

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

MetroCluster and miscellaneous guides

Guide	Content
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

Stretch MetroCluster installation and configuration	• Stretch MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • Configuring the MetroCluster in ONTAP
MetroCluster management	• Understanding the MetroCluster configuration • Switchover, healing, and switchback
Disaster Recovery Guide	• Disaster recovery • Forced switchover • Recovery from a multi-controller or storage failure
MetroCluster Maintenance Guide	• Guidelines for maintenance in a MetroCluster FC configuration • Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches • Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster FC configuration • Expanding a two-node fabric-attached or stretch MetroCluster FC configuration to a four-node MetroCluster configuration. • Expanding a four-node fabric-attached or stretch MetroCluster FC configuration to an eight-node MetroCluster FC configuration.
MetroCluster Upgrade and Expansion Guide	• Upgrading or refreshing a MetroCluster configuration • Expanding a MetroCluster configuration by adding additional nodes
MetroCluster Transition Guide	• Transitioning from a MetroCluster FC configuration to a MetroCluster IP configuration
MetroCluster Upgrade, Transition, and Expansion Guide	• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software

AFF and FAS Documentation Center **Note:** The standard storage shelf maintenance procedures can be used with MetroCluster IP configurations.	• Hot-adding a disk shelf • Hot-removing a disk shelf
Copy-based transition	• Transitioning data from 7-Mode storage systems to clustered storage systems
ONTAP concepts	• How mirrored aggregates work

MetroCluster® Upgrade and Expansion Guide

Choosing an upgrade or refresh method

The upgrade or refresh procedure you use depends on the platform model, scope of the upgrade, and type of MetroCluster configuration.

There are different types of upgrade and refresh procedures.

- Upgrade procedures apply only to the controller modules. The controllers are replaced with a new controller model.

  The storage shelf models are not upgraded.

  - In switchover and switchback procedures, the MetroCluster switchover operation is used to provide nondisruptive service to clients while the controller modules on the partner cluster are upgraded.
  - In an ARL-based controller upgrade procedure, the aggregate relocation operations are used to nondisruptively move data from the old configuration to the new, upgraded configuration.
- Refresh procedures apply to the controllers and the storage shelves.

  In the refresh procedures, new controllers and shelves are added to the MetroCluster configuration, creating a second DR group, and then data is nondisruptively migrated to the new nodes.

  The original controllers are then retired.

Choosing a procedure that does not use aggregate relocation

Type of upgrade or refresh	MetroCluster type	First ONTAP version support	Procedure
• Scope: Platform (controller modules) only • Method: Switchover/switchback	FC	9.8	Upgrading controllers in a MetroCluster FC configuration using switchover and switchback
• Scope: Platform (controller modules) only • Method: Switchover/switchback	IP	9.8	Upgrading controllers in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.8 and later)

• Scope: Platform (controller modules) and storage shelves • Method: Expand the MetroCluster configuration and then remove the old nodes	FC	9.6 and later	Refreshing a four-node MetroCluster FC configuration
• Scope: Platform (controller modules) and storage shelves • Method: Expand the MetroCluster configuration and then remove the old nodes	IP	9.8	Refreshing a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Choosing a procedure using aggregate relocation

Aggregate relocation procedure	MetroCluster type	First ONTAP version support	Procedure
Using `system controller replace` commands	FC	9.8 and later	Using “system controller replace” Commands to Upgrade Controller Hardware Running ONTAP 9.8
Using `system controller replace` commands	FC	9.5 through 9.7	Using “system controller replace” Commands to Upgrade Controller Hardware Running ONTAP 9.5 to ONTAP 9.7
Using manual ARL commands	FC	9.8	Using Aggregate Relocation to Manually Upgrade Controller Hardware Running ONTAP 9.8 and Later
Using manual ARL commands	FC	9.7 and earlier	Upgrading Controllers with Aggregate Relocation to Manually Upgrade Controller Hardware Running ONTAP 9.7 and Earlier

Choosing an upgrade or refresh method

The upgrade or refresh procedure you use depends on the platform model, scope of the upgrade, and type of MetroCluster configuration.

There are different types of upgrade and refresh procedures.

- Upgrade procedures apply only to the controller modules. The controllers are replaced with a new controller model.

  The storage shelf models are not upgraded.

  - In switchover and switchback procedures, the MetroCluster switchover operation is used to provide nondisruptive service to clients while the controller modules on the partner cluster are upgraded.
  - In an ARL-based controller upgrade procedure, the aggregate relocation operations are used to nondisruptively move data from the old configuration to the new, upgraded configuration.
- Refresh procedures apply to the controllers and the storage shelves.

  In the refresh procedures, new controllers and shelves are added to the MetroCluster configuration, creating a second DR group, and then data is nondisruptively migrated to the new nodes.

  The original controllers are then retired.

Choosing a procedure that does not use aggregate relocation

Type of upgrade or refresh	MetroCluster type	First ONTAP version support	Procedure
• Scope: Platform (controller modules) only • Method: Switchover/switchback	FC	9.8	Upgrading controllers in a MetroCluster FC configuration using switchover and switchback
• Scope: Platform (controller modules) only • Method: Switchover/switchback	IP	9.8	Upgrading controllers in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.8 and later)
• Scope: Platform (controller modules) and storage shelves • Method: Expand the MetroCluster configuration and then remove the old nodes	FC	9.6 and later	Refreshing a four-node MetroCluster FC configuration

• Scope: Platform (controller modules) and storage shelves • Method: Expand the MetroCluster configuration and then remove the old nodes	IP	9.8	Refreshing a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Choosing a procedure using aggregate relocation

Aggregate relocation procedure	MetroCluster type	First ONTAP version support	Procedure
Using `system controller replace` commands	FC	9.8 and later	Using “system controller replace” Commands to Upgrade Controller Hardware Running ONTAP 9.8 and Later
Using `system controller replace` commands	FC	9.5 through 9.7	Using “system controller replace” Commands to Upgrade Controller Hardware Running ONTAP 9.5 to ONTAP 9.7
Using manual ARL commands	FC	9.8	Manually Upgrade Controller Hardware Running ONTAP 9.8 and Later
Using manual ARL commands	FC	9.7 and earlier	Manually Upgrade Controller Hardware Running ONTAP 9.7 and Earlier

Upgrading controllers in a MetroCluster FC configuration using switchover and switchback

You can use the MetroCluster switchover operation to provide nondisruptive service to clients while the controller modules on the partner cluster are upgraded. Other components (such as storage shelves or switches) cannot be upgraded as part of this procedure.

About this task

- You can use this procedure only for controller upgrade.

  Other components in the configuration, such as storage shelves or switches, cannot be upgraded at the same time.

* You can use this procedures with certain ONTAP versions:
  * Two-node configurations are supported in ONTAP 9.3 and later.
  * Four and eight node configurations are supported in ONTAP 9.8 and later.

    Do not use this procedure on four- or eight-node configurations running ONTAP versions prior to 9.8.
* Your original and new platforms must be compatible and supported.

  NetApp Hardware Universe

  > If the original or new platforms are 8020 systems using ports 1c / 1d in FC-VI mode, contact technical support.
* This procedure applies to controller modules in a MetroCluster FC configuration (a two-node stretch MetroCluster or a two or four-node fabric-attached MetroCluster configuration).
* All controllers in the configuration should be upgraded during the same maintenance period.

  Operating the MetroCluster configuration with different controller types is not supported outside of this maintenance activity.
* The supported upgrade path depends on the original platform model.

  Platform models with internal shelves are not supported.

Old platform model	New platform model
• FAS80xx • FAS8200	• FAS8300 • FAS8700
• AFF A300	• AFF A400 • AFF A700

* Mapping of storage, FC and Ethernet connections between original nodes and new nodes in advance is recommended.
* If the new platform has fewer slots than the original system, or if it has fewer or different types of ports, you might need to add an adapter to the new system.

  For more information, see the NetApp Hardware Universe

The following example names are used in this procedure:

* site_A
  * Before upgrade:
    * node_A_1-old
    * node_A_2-old
  * After upgrade:
    * node_A_1-new

        ▪ node_A_2-new

- site_B
  - Before upgrade:
    - node_B_1-old
    - node_B_2-old
  - After upgrade:
    - node_B_1-new
    - node_B_2-new

Preparing for the upgrade

Before making any changes to the existing MetroCluster configuration, you must check the health of the configuration, prepare the new platforms, and perform other miscellaneous tasks.

Verifying the health of the MetroCluster configuration

You must verify the health and connectivity of the MetroCluster configuration prior to performing the upgrade.

Steps

1. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the nodes are multipathed:
      `node run -node node-name sysconfig -a`

      You should issue this command for each node in the MetroCluster configuration.
   b. Verify that there are no broken disks in the configuration:

      `storage disk show -broken`

      You should issue this command on each node in the MetroCluster configuration.
   c. Check for any health alerts:

      `system health alert show`

      You should issue this command on each cluster.
   d. Verify the licenses on the clusters:

      `system license show`

      You should issue this command on each cluster.
   e. Verify the devices connected to the nodes:

      `network device-discovery show`

      You should issue this command on each cluster.
   f. Verify that the time zone and time are set correctly on both sites:

```
cluster date show
```

You should issue this command on each cluster. You can use the `cluster date` commands to configure the time and time zone.

2. Check for any health alerts on the switches (if present):

   ```
   storage switch show
   ```

   You should issue this command on each cluster.

3. Confirm the operational mode of the MetroCluster configuration and perform a MetroCluster check.
   a. Confirm the MetroCluster configuration and that the operational mode is normal:

      ```
      metrocluster show
      ```

   b. Confirm that all expected nodes are shown:

      ```
      metrocluster node show
      ```

   c. Issue the following command:

      ```
      metrocluster check run
      ```

   d. Display the results of the MetroCluster check:

      ```
      metrocluster check show
      ```

4. Check the MetroCluster cabling with the Config Advisor tool.
   a. Download and run Config Advisor.

      NetApp Downloads: Config Advisor

   b. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Mapping ports from the old nodes to the new nodes

You must plan the mapping of the LIFs on physical ports on the old nodes to the physical ports on the new nodes.

About this task

When the new node is first booted during the upgrade process, it will replay the most recent configuration of the old node it is replacing. When you boot node_A_1-new, ONTAP attempts to host LIFs on the same ports that were used on node_A_1-old. Therefore, as part of the upgrade you must adjust the port and LIF configuration so it is compatible with that of the old node. During the upgrade procedure, you will perform steps on both the old and new nodes to ensure correct cluster, management, and data LIF configuration.

The following table shows examples of configuration changes related to the port requirements of the new nodes.

Cluster interconnect physical ports

Old controller	New controller	Required action
e0a, e0b	e3a, e3b	No matching port. After upgrade, you must recreate cluster ports.
e0c, e0d	e0a,e0b,e0c,e0d	e0c and e0d are matching ports. You do not have to change the configuration, but after upgrade you can spread your cluster LIFs across the available cluster ports.

Steps

1. Determine what physical ports are available on the new controllers and what LIFs can be hosted on the ports.

   The controller's port usage depends on the platform module and which switches you will use in the MetroCluster IP configuration. You can gather the port usage of the new platforms from the NetApp Hardware Universe.

   Also identify the FC-VI card slot usage.

2. Plan your port usage and, if desired, fill in the following tables for reference for each of the new nodes.

   You will refer to the table as you carry out the upgrade procedure.

	node_A_1-old			**node_A_1-new**		
LIF	**Ports**	**IPspaces**	**Broadcast domains**	**Ports**	**IPspaces**	**Broadcast domains**
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Node management						
Cluster management						
Data 1						
Data 2						
Data 3						

Data 4						
SAN						
Intercluster port						

Gathering information before the upgrade

Before upgrading, you must gather information for each of the nodes, and, if necessary, adjust the network broadcast domains, remove any VLANs and interface groups, and gather encryption information.

About this task

This task is performed on the existing MetroCluster FC configuration.

Steps

1. Label the cables for the existing controllers, to allow easy identification of cables when setting up the new controllers.
2. Gather the system IDs of the nodes in the MetroCluster configuration:

   ```
   metrocluster node show -fields node-systemid,dr-partner-systemid
   ```

   During the replacement procedure you will replace these system IDs with the system IDs of the new controller modules.

   In this example for a four-node MetroCluster FC configuration, the following old system IDs are retrieved:

   - node_A_1-old: 4068741258
   - node_A_2-old: 4068741260
   - node_B_1-old: 4068741254
   - node_B_2-old: 4068741256

```
metrocluster-siteA::> metrocluster node show -fields node-
systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-
systemid
dr-group-id   cluster                       node
node-systemid          ha-partner-systemid     dr-partner-systemid
dr-auxiliary-systemid
-----------        ------------------------- ------------------
-------------                   -------------------
-------------------              ---------------------
1                    Cluster_A                  Node_A_1-old
4068741258              4068741260                        4068741256
4068741256
1                    Cluster_A                    Node_A_2-old
4068741260              4068741258                        4068741254
4068741254
1                    Cluster_B                    Node_B_1-old
4068741254              4068741256                         4068741258
4068741260
1                    Cluster_B                    Node_B_2-old
4068741256              4068741254                        4068741260
4068741258
4 entries were displayed.
```

In this example for a two-node MetroCluster FC configuration, the following old system IDs are retrieved:

- node_A_1: 4068741258
- node_B_1: 4068741254

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1-old  4068741258    4068741254
1           Cluster_B  node_B_1-old  -             -
2 entries were displayed.
```

3. Gather port and LIF information for each node.

   You should gather the output of the following commands for each node:

   - `network interface show -role cluster,node-mgmt`
   - `network port show -node` *`node-name`* `-type physical`
   - `network port vlan show -node` *`node-name`*

- `network port ifgrp show -node node_name -instance`
- `network port broadcast-domain show`
- `network port reachability show -detail`
- `network ipspace show`
- `volume show`
- `storage aggregate show`
- `system node run -node node-name sysconfig -a`

4. If the MetroCluster nodes are in a SAN configuration, collect the relevant information.

   You should gather the output of the following commands:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. If the root volume is encrypted, collect and save the passphrase used for key-manager:

   `security key-manager backup show`

6. If the MetroCluster nodes are using encryption for volumes or aggregates, copy information about the keys and passphrases.

   For additional information, see Backing up onboard key management information manually.

   a. If Onboard Key Manager is configured:

      `security key-manager onboard show-backup`

      You will need the passphrase later in the upgrade procedure.

   b. If enterprise key management (KMIP) is configured, issue the following commands:

      `security key-manager external show -instance`

      `security key-manager key query`

Removing the existing configuration from the Tiebreaker or other monitoring software

If the existing configuration is monitored with the MetroCluster Tiebreaker configuration or other third-party applications (for example, ClusterLion) that can initiate a switchover, you must remove the MetroCluster configuration from the Tiebreaker or other software prior to transition.

Steps

1. Remove the existing MetroCluster configuration from the Tiebreaker software.

   Removing MetroCluster configurations

2. Remove the existing MetroCluster configuration from any third-party application that can initiate switchover.

   Refer to the documentation for the application.

Sending a custom AutoSupport message prior to maintenance

Before performing the maintenance, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

About this task

This task must be performed on each MetroCluster site.

Steps

1. To prevent automatic support case generation, send an Autosupport message to indicate maintenance is underway.
   a. Issue the following command:

      `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

      `maintenance-window-in-hours` specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

      `system node autosupport invoke -node * -type all -message MAINT=end`

   b. Repeat the command on the partner cluster.

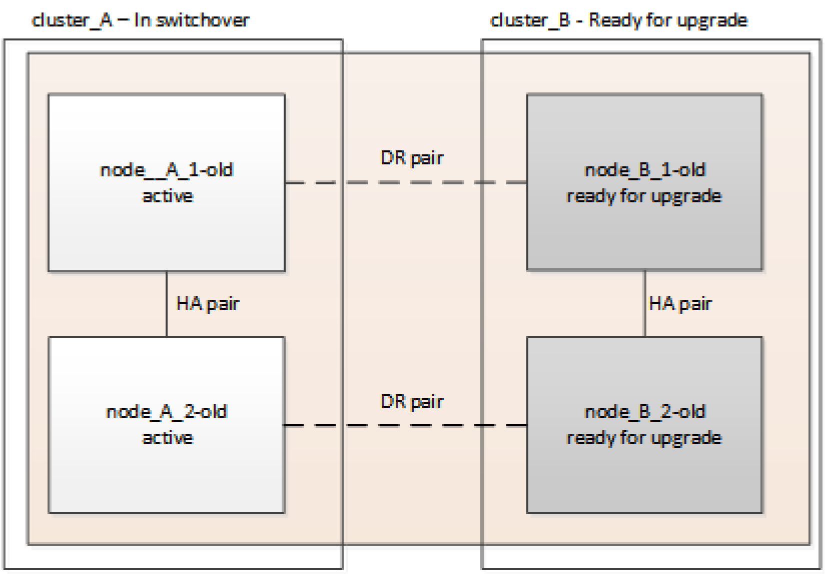
Switching over the MetroCluster configuration

You must switch over the configuration to site_A so that the platforms on site_B can be upgraded.

About this task

This task must be performed on site_A.

After completing this task, cluster_A is active and serving data for both sites. cluster_B is inactive, and ready to begin the upgrade process, as shown in the following illustration.



Steps

1. Switch over the MetroCluster configuration to site_A so that site_B's nodes can be upgraded:
   a. Issue the following command on cluster_A:

      `metrocluster switchover -controller-replacement true`

      The operation can take several minutes to complete.

   b. Monitor the switchover operation:

      `metrocluster operation show`

   c. After the operation is complete, confirm that the nodes are in switchover state:

      `metrocluster show`

   d. Check the status of the MetroCluster nodes:

      `metrocluster node show`

2. Heal the data aggregates.
   a. Heal the data aggregates:

      `metrocluster heal data-aggregates`

   b. Confirm the heal operation is complete by running the `metrocluster operation show` command on the healthy cluster:

```
cluster_A::> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 7/29/2020 20:54:41
   End Time: 7/29/2020 20:54:42
     Errors: -
```

3. Heal the root aggregates.
   a. Heal the data aggregates:

      `metrocluster heal root-aggregates`

   b. Confirm the heal operation is complete by running the `metrocluster operation show` command on the healthy cluster:

```
cluster_A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2020 20:58:41
   End Time: 7/29/2020 20:59:42
     Errors: -
```

Preparing the network configuration of the old controllers

To ensure that the networking resumes cleanly on the new controllers, you must move LIFs to a common port and then remove the networking configuration of the old controllers.

About this task

- This task must be performed on each of the old nodes.
- You will use the information gathered in Mapping ports from the old nodes to the new nodes.

Steps

1. Boot the old nodes and then log in to the nodes:

   `boot_ontap`

2. Assign the home port of all data LIFs on the old controller to a common port that is the same on both the old and new controller modules.
   a. Display the LIFs:

      `network interface show`

      All data LIFS including SAN and NAS will be admin up and operationally down since those are up at switchover site (cluster_A).

   b. Review the output to find a common physical network port that is the same on both the old and new controllers that is not used as a cluster port.

For example, e0d is a physical port on old controllers and is also present on new controllers. e0d is not used as a cluster port or otherwise on the new controllers.

For port usage for platform models, see the NetApp Hardware Universe

c. Modify all data LIFS to use the common port as the home port:

`network interface modify -vserver svm-name -lif data-lif -home-port port-id`

In the following example, this is "e0d".

For example:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Modify broadcast domains to remove vlan and physical ports that need to be deleted:

`broadcast-domain remove-ports -broadcast-domain broadcast-domain-name -ports node-name:port-id`

Repeat this step for all VLAN and physical ports.

4. Remove any VLAN ports using cluster ports as member ports and ifgrps using cluster ports as member ports.

a. Delete VLAN ports:

`network port vlan delete -node node-name -vlan-name portid-vlandid`

For example:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Remove physical ports from the interface groups:

`network port ifgrp remove-port -node node-name -ifgrp interface-group-name -port portid`

For example:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

c. Remove VLAN and interface group ports from broadcast domain::

`network port broadcast-domain remove-ports -ipspace ipspace -broadcast -domain broadcast-domain-name -ports nodename:portname,nodename:portname,..`

d. Modify interface group ports to use other physical ports as member as needed.:

```
ifgrp add-port -node node-name -ifgrp interface-group-name -port port-id
```

5. Halt the nodes:

   ```
   halt -inhibit-takeover true -node node-name
   ```

   This step must be performed on both nodes.

Removing the old platforms

The old controllers must be removed from the configuration.

About this task

This task is performed on site_B.

Steps

1. Connect to the serial console of the old controllers (node_B_1-old and node_B_2-old) at site_B and verify it is displaying the LOADER prompt.
2. Disconnect the storage and network connections on node_B_1-old and node_B_2-old and label the cables so they can be reconnected to the new nodes.
3. Disconnect the power cables from node_B_1-old and node_B_2-old.
4. Remove the node_B_1-old and node_B_2-old controllers from the rack.

Configuring the new controllers

You must rack and install the controllers, perform required setup in Maintenance mode, and then boot the controllers, and verify the LIF configuration on the controllers.

Setting up the new controllers

You must rack and cable the new controllers.

Steps

1. Plan out the positioning of the new controller modules and storage shelves as needed.

   The rack space depends on the platform model of the controller modules, the switch types, and the number of storage shelves in your configuration.

2. Properly ground yourself.
3. Install the controller modules in the rack or cabinet.

   AFF and FAS Documentation Center

4. If the new controller modules did not come with FC-VI cards of their own and if FC-VI cards from old controllers are compatible on new controllers, swap FC-VI cards and install those in correct slots.

   See the NetApp Hardware Universe for slot info for FC-VI cards.

5. Cable the controllers' power, serial console and management connections as described in the *MetroCluster Installation and Configuration Guides*.

Do not connect any other cables that were disconnected from old controllers at this time.

AFF and FAS Documentation Center

6. Power up the new nodes and press Ctrl-C when prompted to display the LOADER prompt.

Netbooting the new controllers

After you install the new nodes, you need to netboot to ensure the new nodes are running the same version of ONTAP as the original nodes. The term netboot means you are booting from an ONTAP image stored on a remote server. When preparing for netboot, you must put a copy of the ONTAP 9 boot image onto a web server that the system can access.

This task is performed on each of the new controller modules.

Steps

1. Access the NetApp Support Site to download the files used for performing the netboot of the system.
2. Download the appropriate ONTAP software from the software download section of the NetApp Support Site and store the ontap-version_image.tgz file on a web-accessible directory.
3. Go to the web-accessible directory and verify that the files you need are available.

If the platform model is…	Then…
FAS/AFF8000 series systems	Extract the contents of the ontap-version_image.tgzfile to the target directory: tar -zxvf ontap-version_image.tgz NOTE: If you are extracting the contents on Windows, use 7-Zip or WinRAR to extract the netboot image. Your directory listing should contain a netboot folder with a kernel file:netboot/kernel
All other systems	Your directory listing should contain a netboot folder with a kernel file: ontap-version_image.tgz You do not need to extract the ontap-version_image.tgz file.

4. At the LOADER prompt, configure the netboot connection for a management LIF:
   - If IP addressing is DHCP, configure the automatic connection:

     `ifconfig e0M -auto`

   - If IP addressing is static, configure the manual connection:

     `ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway`

5. Perform the netboot.
   - If the platform is an 80xx series system, use this command:

     `netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`

◦ If the platform is any other system, use the following command:

```
netboot http://web_server_ip/path_to_web-accessible_directory/ontap-
version_image.tgz
```

6. From the boot menu, select option **(7) Install new software first** to download and install the new software image to the boot device.

```
Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
```

7. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL of the image file: `http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

```
Enter username/password if applicable, or press Enter to continue.
```

8. Be sure to enter `n` to skip the backup recovery when you see a prompt similar to the following:

```
Do you want to restore the backup configuration now? {y|n}
```

9. Reboot by entering `y` when you see a prompt similar to the following:

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n}
```

Clearing the configuration on a controller module

Before using a new controller module in the MetroCluster configuration, you must clear the existing configuration.

Steps

1. If necessary, halt the node to display the LOADER prompt:

```
halt
```

2. At the LOADER prompt, set the environmental variables to default values:

```
set-defaults
```

3. Save the environment:

```
saveenv
```

4. At the LOADER prompt, launch the boot menu:

   `boot_ontap menu`

5. At the boot menu prompt, clear the configuration:

   `wipeconfig`

   Respond `yes` to the confirmation prompt.

   The node reboots and the boot menu is displayed again.

6. At the boot menu, select option **5** to boot the system into Maintenance mode.

   Respond `yes` to the confirmation prompt.

Restoring the HBA configuration

Depending on the presence and configuration of HBA cards in the controller module, you need to configure them correctly for your site's usage.

Steps

1. In Maintenance mode configure the settings for any HBAs in the system:

   a. Check the current settings of the ports: `ucadmin show`

   b. Update the port settings as needed.

If you have this type of HBA and desired mode…	Use this command…
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
FC target	`fcadmin config -t target` *`adapter-name`*
FC initiator	`fcadmin config -t initiator` *`adapter-name`*

2. Exit Maintenance mode:

   `halt`

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

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

   `boot_ontap maint`

4. Verify the changes you made:

If you have this type of HBA…	Use this command…
CNA	`ucadmin show`
FC	`fcadmin show`

Setting the HA state on the new controllers and chassis

You must verify the HA state of the controllers and chassis, and, if necessary, update the state to match your system configuration.

Steps

1. In Maintenance mode, display the HA state of the controller module and chassis:

   `ha-config show`

   The HA state for all components should be mcc.

If the MetroCluster configuration has…	The HA state should be…
Two nodes	mcc-2n
Four or eight nodes	mcc

2. If the displayed system state of the controller is not correct, set the HA state for the controller module and chassis:

If the MetroCluster configuration has…	Issue these commands…
Two nodes	`ha-config modify controller mcc-2n` `ha-config modify chassis mcc-2n`
Four or eight nodes	`ha-config modify controller mcc` `ha-config modify chassis mcc`

Reassigning root aggregate disks

Reassign the root aggregate disks to the new controller module, using the sysids gathered earlier

About this task

This task is performed in Maintenance mode.

The old system IDs were identified in Gathering information before the upgrade.

The examples in this procedure use controllers with the following system IDs:

Node	Old system ID	New system ID
node_B_1	4068741254	1574774970

Steps

1. Cable all other connections to the new controller modules (FC-VI, storage, cluster interconnect, etc.).
2. Halt the system and boot to Maintenance mode from the LOADER prompt:

   `boot_ontap maint`

3. Display the disks owned by node_B_1-old:

   `disk show -a`

   The command output shows the system ID of the new controller module (1574774970). However, the root aggregate disks are still owned by the old system ID (4068741254). This example does not show drives owned by other nodes in the MetroCluster configuration.

```
*> disk show -a
Local System ID: 1574774970

  DISK         OWNER                     POOL   SERIAL NUMBER    HOME
DR HOME
------------   -------------             -----  -------------
-------------             -------------
...
rr18:9.126L44 node_B_1-old(4068741254)   Pool1  PZHYN0MD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L49 node_B_1-old(4068741254)   Pool1  PPG3J5HA
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L21 node_B_1-old(4068741254)   Pool1  PZHTDSZD
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L2  node_B_1-old(4068741254)   Pool0  S0M1J2CF
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:8.126L3  node_B_1-old(4068741254)   Pool0  S0M0CQM5
node_B_1-old(4068741254)  node_B_1-old(4068741254)
rr18:9.126L27 node_B_1-old(4068741254)   Pool0  S0M1PSDW
node_B_1-old(4068741254)  node_B_1-old(4068741254)
...
```

4. Reassign the root aggregate disks on the drive shelves to the new controller:

   `disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

   The following example shows reassignment of drives:

```
*> disk reassign -s 4068741254 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? Jul 14 19:23:49
[localhost:config.bridge.extra.port:error]: Both FC ports of FC-to-SAS
bridge rtp-fc02-41-rr18:9.126L0 S/N [FB7500N107692] are attached to this
controller.
y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 4068741254.
Do you want to continue (y/n)? y
```

5. Check that all disks are reassigned as expected:

   `disk show`

```
*> disk show
Local System ID: 1574774970

  DISK        OWNER                        POOL   SERIAL NUMBER   HOME
DR HOME
------------  -------------                -----  -------------
-------------             -------------
rr18:8.126L18 node_B_1-new(1574774970)   Pool1  PZHYN0MD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L49 node_B_1-new(1574774970)   Pool1  PPG3J5HA
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L21 node_B_1-new(1574774970)   Pool1  PZHTDSZD
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L2  node_B_1-new(1574774970)   Pool0  S0M1J2CF
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:9.126L29 node_B_1-new(1574774970)   Pool0  S0M0CQM5
node_B_1-new(1574774970)  node_B_1-new(1574774970)
rr18:8.126L1  node_B_1-new(1574774970)   Pool0  S0M1PSDW
node_B_1-new(1574774970)  node_B_1-new(1574774970)
*>
```

6. Display the aggregate status:

   `aggr status`

```
*> aggr status
           Aggr            State       Status           Options
aggr0_node_b_1-root    online      raid_dp, aggr    root, nosnap=on,
                           mirrored
mirror_resync_priority=high(fixed)
                           fast zeroed
                           64-bit
```

7. Repeat the above steps on the partner node (node_B_2-new).

Booting up the new controllers

You must reboot the controllers from the boot menu to update the controller flash image. Additional steps are required if encryption is configured.

About this task

This task must be performed on all the new controllers.

Steps

1. Halt the node:

   `halt`

2. If external key manager is configured, set the related bootargs:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`*

   `setenv bootarg.kmip.init.interface` *`interface-id`*

3. Display the boot menu:

   `boot_ontap menu`

4. If root encryption is used, issue the boot menu command for your key management configuration.

If you are using…	Issue this command at the boot menu prompt…
Onboard key management	`recover_onboard_keymanager`
External key management	`recover_external_keymanager`

5. If autoboot is enabled, interrupt autoboot by pressing control-C.
6. From the boot menu, run option (6).

   > Option 6 will reboot the node twice before completing.

   Respond `y` to the system id change prompts. Wait for the second reboot messages:

   ```
   Successfully restored env file from boot media...

   Rebooting to load the restored env file...
   ```

7. Double-check that the partner-sysid is correct:

   `printenv partner-sysid`

   If the partner-sysid is not correct, set it:

   `setenv partner-sysid` *`partner-sysID`*

8. If root encryption is used, issue the boot menu command again for your key management configuration.

If you are using…	Issue this command at the boot menu prompt…
Onboard key management	`recover_onboard_keymanager`
External key management	`recover_external_keymanager`

You may need to issue the recover_xxxxxxxx_keymanager command and option 6 at the boot menu prompt multiple times until the nodes completely boot.

1. Boot the nodes:

   `boot_ontap`

2. Wait for the replaced nodes to boot up.

   If either node is in takeover mode, perform a giveback using the `storage failover giveback` command.

3. Verify that all ports are in a broadcast domain:

   a. View the broadcast domains:

      `network port broadcast-domain show`

   b. Add any ports to a broadcast domain as needed.

      Adding or removing ports from a broadcast domain

   c. Add the physical port that will host the intercluster LIFs to the corresponding Broadcast domain.

d. Modify intercluster LIFs to use the new physical port as home port.

e. After the intercluster LIFs are up, check the cluster peer status and re-establish cluster peering as needed.

   You may need to reconfigure cluster peering.

   Creating a cluster peer relationship

f. Recreate VLANs and interface groups as needed.

   VLAN and interface group membership might be different than that of the old node.

   Creating a VLAN

   Combining physical ports to create interface groups

4. If encryption is used, restore the keys using the correct command for your key management configuration.

If you are using…	Use this command…
Onboard key management	`security key-manager onboard sync` For more information, see Restoring onboard key management encryption keys.
External key management	`security key-manager external restore -vserver` *`SVM`* `-node` *`node`* `-key-server` *`host_name|IP_address:port`* `-key-id key_id -key-tag key_tag` *`node-name`* For more information, see Restoring external key management encryption keys.

Verifying LIF configuration

Verify that LIFs are hosted on appropriate node/ports prior to switchback. The following steps need to be performed

About this task

This task is performed on site_B, where the nodes have been booted up with root aggregates.

Steps

1. Verify that LIFs are hosted on the appropriate node and ports prior to switchback.

   a. Change to the advanced privilege level:

   ```
   set -privilege advanced
   ```

   b. Override the port configuration to ensure proper LIF placement:

   ```
   vserver config override -command "network interface modify" -vserver
   vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
   ```

new_node_name"

When entering the `network interface modify` command within the `vserver config override` command, you cannot use the tab autocomplete feature. You can create the `network interface modify` using autocomplete and then enclose it in the `vserver config override` command.

c. Return to the admin privilege level:
`set -privilege admin`

2. Revert the interfaces to their home node:

```
network interface revert * -vserver vserver-name
```

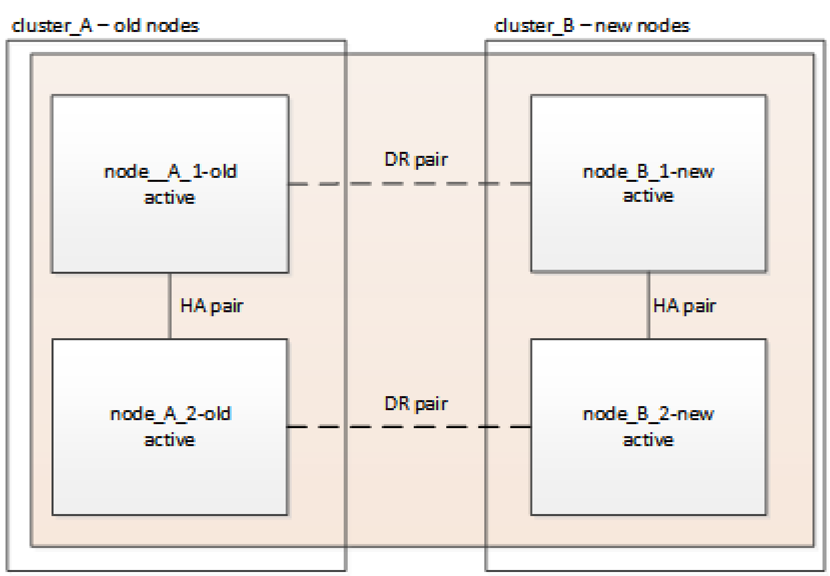
Perform this step on all SVMs as required.

Switching back the MetroCluster configuration

After the new controllers have been configured, you switch back the MetroCluster configuration to return the configuration to normal operation.

About this task

In this task, you will perform the switchback operation, returning the MetroCluster configuration to normal operation. The nodes on site_A are still awaiting upgrade.



Steps

1. Issue the `metrocluster node show` command on site_B and check the output.
   a. Verify that the new nodes are represented correctly.
   b. Verify that the new nodes are in "Waiting for switchback state."
2. Switchback the cluster:

```
metrocluster switchback
```

3. Check the progress of the switchback operation:

```
metrocluster show
```

The switchback operation is still in progress when the output displays `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

The switchback operation is complete when the output displays `normal`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

If a switchback takes a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command. This command is at the advanced privilege level.

Checking the health of the MetroCluster configuration

After upgrading the controller modules you must verify the health of the MetroCluster configuration.

About this task

This task can be performed on any node in the MetroCluster configuration.

Steps

1. Verify the operation of the MetroCluster configuration:
   a. Confirm the MetroCluster configuration and that the operational mode is normal:

      ```
      metrocluster show
      ```

   b. Perform a MetroCluster check:

      ```
      metrocluster check run
      ```

c. Display the results of the MetroCluster check:

```
metrocluster check show
```

Upgrading the nodes on cluster_A

You must repeat the upgrade tasks on cluster_A.

Step

1. Repeat the steps to upgrade the nodes on cluster_A, beginning with Preparing for the upgrade.

   As you perform the tasks, all example references to the clusters and nodes are reversed. For example, when the example is given to switchover from cluster_A, you will switchover from cluster_B.

Sending a custom AutoSupport message after maintenance

After completing the upgrade, you should send an AutoSupport message indicating the end of maintenance, so automatic case creation can resume.

Step

1. To resume automatic support case generation, send an Autosupport message to indicate that the maintenance is complete.
   a. Issue the following command:

      ```
      system node autosupport invoke -node * -type all -message MAINT=end
      ```

   b. Repeat the command on the partner cluster.

Restoring Tiebreaker monitoring

If the MetroCluster configuration was previously configured for monitoring by the Tiebreaker software, you can restore the Tiebreaker connection.

1. Use the steps in Adding MetroCluster configurations in the *MetroCluster Tiebreaker Installation and Configuration Guide*.

Upgrading controllers in a MetroCluster IP configuration using switchover and switchback (ONTAP 9.8 and later)

Starting with ONTAP 9.8, you can use the MetroCluster switchover operation to provide nondisruptive service to clients while the controller modules on the partner cluster are upgraded. Other components (such as storage shelves or switches) cannot be upgraded as part of this procedure.

About this task

- The platforms must be running ONTAP 9.8 or later.
- This procedure applies to controller modules in a MetroCluster IP configuration.
- The supported upgrade path depends on the original platform model.

Platform models with internal shelves are not supported.

Old platform model	New platform model
• AFF A320	• AFF A400
• FAS8200	• FAS9000 • FAS8300 • FAS8700

AFF A320 platform models are not supported for upgrade when using BES-53248 IP switches.

- All controllers in the configuration should be upgraded during the same maintenance period.

  Operating the MetroCluster configuration with different controller types is not supported outside of this maintenance activity.

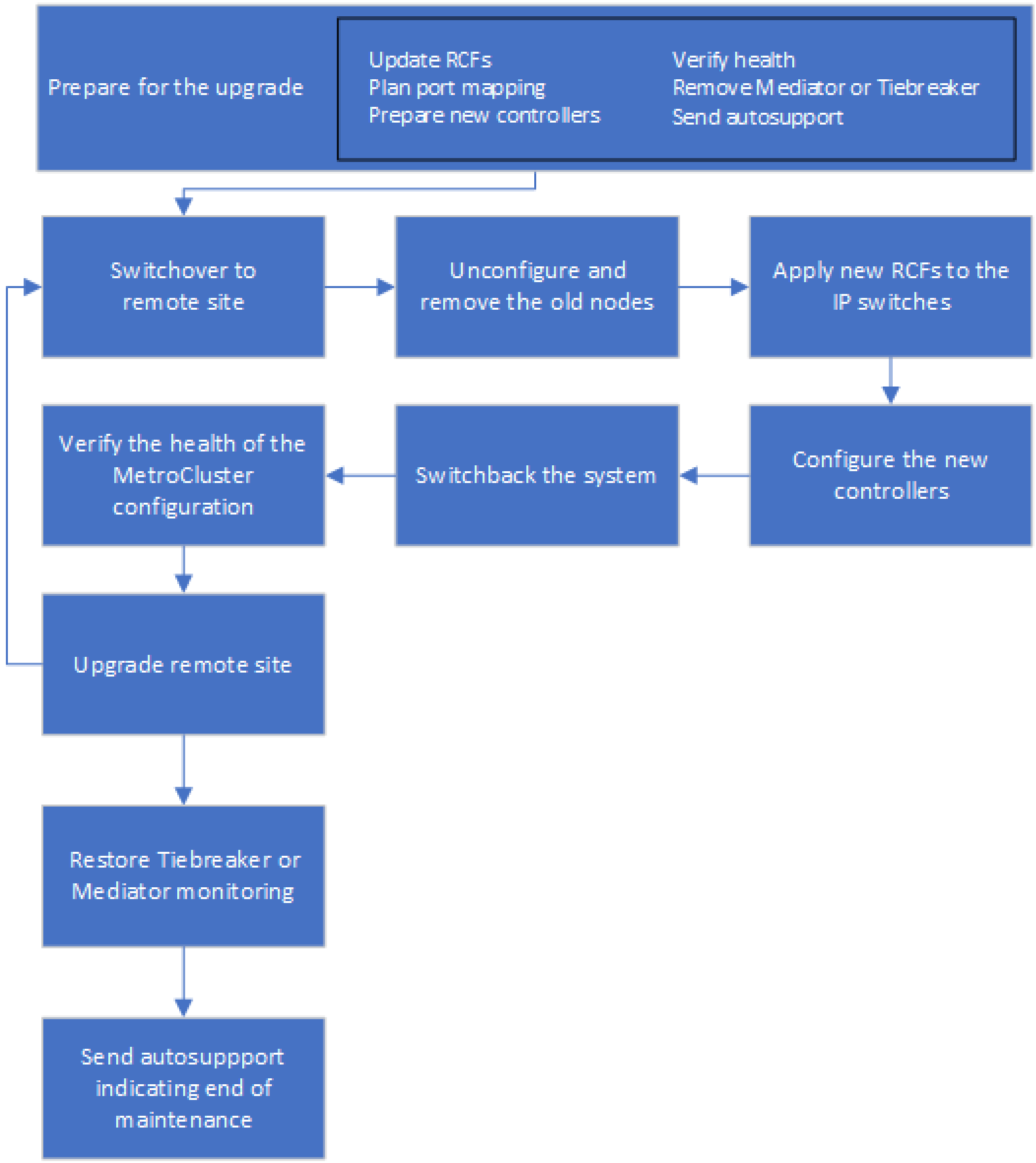
- The new platform must be a different model than the original platform.
- The IP switches must be running a supported firmware version.
- If the new platform has fewer slots than the original system, or if it has fewer or different types of ports, you might need to add an adapter to the new system.

  For more information, see the NetApp Hardware Universe.

- You will reuse the IP addresses, netmasks, and gateways of the original platforms on the new platforms.
- The following example names are used in this procedure:
  - site_A
    - Before upgrade:
      - node_A_1-old
      - node_A_2-old
    - After upgrade:
      - node_A_1-new
      - node_A_2-new
  - site_B
    - Before upgrade:
      - node_B_1-old
      - node_B_2-old
    - After upgrade:
      - node_B_1-new
      - node_B_2-new

Workflow for upgrading controllers in an MetroCluster IP configuration

You can use the workflow diagram to help you plan the upgrade tasks.



Preparing for the upgrade

Before making any changes to the existing MetroCluster configuration, you must check the health of the configuration, prepare the new platforms, and perform other miscellaneous tasks.

Updating the MetroCluster switch RCF files before upgrading controllers

Depending on the old platform models, or if switch configuration is not on the minimum version, or if you want to change VLAN IDs used by the back-end MetroCluster connections, you must update the switch RCF files before you begin the platform upgrade procedure.

About this task

You must update the RCF file in the following scenarios:

- For certain platform models, the switches must be using a supported VLAN ID for the back-end

MetroCluster IP connections. If the old or new platform models are in the following table, **and not** using a supported VLAN ID, you must update the switch RCF files.

> The local cluster connections can use any VLAN, they do not need to be in the given range.

Platform model (old or new)	Supported VLAN IDs
• AFF A400	• 10 • 20 • Any value in the range 101 to 4096 inclusive.

- The switch configuration was not configured with minimum supported RCF version:

Switch model	Required RCF file version
Cisco 3132Q-V	1.7 or later
Cisco 3232C	1.7 or later
Broadcom BES-53248	1.3 or later

- You want to change the VLAN configuration.

  The VLAN ID range is 101 to 4096 inclusive.

The switches at site_A will be upgraded when the controllers on site_A are upgraded.

Steps

1. Prepare the IP switches for the application of the new RCF files.

   Follow the steps in the section for your switch vendor from the MetroCluster IP Installation and Configuration Guide.

   - Resetting the Broadcom IP switch to factory defaults
   - Resetting the Cisco IP switch to factory defaults

2. Download and install the RCF files.

   Follow the steps in the MetroCluster IP Installation and Configuration Guide.

   - Downloading and installing the Broadcom RCF files
   - Downloading and installing the Cisco IP RCF files

Mapping ports from the old nodes to the new nodes

You must verify that the physical ports on node_A_1-old map correctly to the physical ports on node_A_1-new, which will allow node_A_1-new to communicate with other nodes in the cluster and with the network after the upgrade.

About this task

When the new node is first booted during the upgrade process, it will replay the most recent configuration of the old node it is replacing. When you boot node_A_1-new, ONTAP attempts to host LIFs on the same ports that were used on node_A_1-old. Therefore, as part of the upgrade you must adjust the port and LIF configuration so it is compatible with that of the old node. During the upgrade procedure, you will perform steps on both the old and new nodes to ensure correct cluster, management, and data LIF configuration.

The following table shows examples of configuration changes related to the port requirements of the new nodes.

Cluster interconnect physical ports		
Old controller	**New controller**	**Required action**
e0a, e0b	e3a, e3b	No matching port. After upgrade, you must recreate cluster ports.
e0c, e0d	e0a,e0b,e0c,e0d	e0c and e0d are matching ports. You do not have to change the configuration, but after upgrade you can spread your cluster LIFs across the available cluster ports.

Steps

1. Determine what physical ports are available on the new controllers and what LIFs can be hosted on the ports.

   The controller's port usage depends on the platform module and which switches you will use in the MetroCluster IP configuration. You can gather the port usage of the new platforms from the NetApp Hardware Universe.

2. Plan your port usage and fill in the following tables for reference for each of the new nodes.

   You will refer to the table as you carry out the upgrade procedure.

	node_A_1-old			**node_A_1-new**		
LIF	**Ports**	**IPspaces**	**Broadcast domains**	**Ports**	**IPspaces**	**Broadcast domains**
Cluster 1						
Cluster 2						
Cluster 3						
Cluster 4						
Node management						

Cluster management						
Data 1						
Data 2						
Data 3						
Data 4						
SAN						
Intercluster port						

Netbooting the new controllers

After you install the new nodes, you need to netboot to ensure the new nodes are running the same version of ONTAP as the original nodes. The term netboot means you are booting from an ONTAP image stored on a remote server. When preparing for netboot, you must put a copy of the ONTAP 9 boot image onto a web server that the system can access.

Steps

1. Netboot the new controllers:
   a. Access the NetApp Support Site to download the files used for performing the netboot of the system.
   b. Download the appropriate ONTAP software from the software download section of the NetApp Support Site and store the `ontap-version_image.tgz` file on a web-accessible directory.
   c. Change to the web-accessible directory and verify that the files you need are available.

If the platform model is…	Then…

FAS/AFF8000 series systems	Extract the contents of the `ontap-version_image.tgz` file to the target directory:
	
	`tar -zxvf ontap-version_image.tgz`
	
	ⓘ If you are extracting the contents on Windows, use 7-Zip or WinRAR to extract the netboot image. Your directory listing should contain a netboot folder with a kernel file:netboot/kernel
	
	Your directory listing should contain a netboot folder with a kernel file:
	
	`netboot/kernel`

All other systems	Your directory listing should contain a netboot folder with a kernel file: `_ontap-version_image.tgz` You do not need to extract the `_ontap-version_image.tgz` file.

d. At the LOADER prompt, configure the netboot connection for a management LIF:

If IP addressing is…	Then…
DHCP	Configure the automatic connection: `ifconfig e0M -auto`
Static	Configure the manual connection: `ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway`

e. Perform the netboot.

If the platform model is…	Then…
FAS/AFF8000 series systems	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`

All other systems	`netboot http://_web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

f. From the boot menu, select option **(7) Install new software first** to download and install the new software image to the boot device.

   Disregard the following message:

   `"This procedure is not supported for Non-Disruptive Upgrade on an HA pair"`. It applies to nondisruptive upgrades of software, not to upgrades of controllers.

g. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL of the image file:

   http://*web_server_ip/path_to_web-accessible_directory/ontap-version*_image.tgz

h. Enter the user name and password if applicable, or press Enter to continue.

i. Be sure to enter `n` to skip the backup recovery when you see a prompt similar to the following:

```
Do you want to restore the backup configuration now? {y|n} **n**
```

j. Reboot by entering **`y`** when you see a prompt similar to the following:

```
The node must be rebooted to start using the newly installed
software. Do you want to reboot now? {y|n}
```

Clearing the configuration on a controller module

Before using a new controller module in the MetroCluster configuration, you must clear the existing configuration.

Steps

1. If necessary, halt the node to display the LOADER prompt:

   `halt`

2. At the LOADER prompt, set the environmental variables to default values:

   `set-defaults`

3. Save the environment:

   `saveenv`

4. At the LOADER prompt, launch the boot menu:

   `boot_ontap menu`

5. At the boot menu prompt, clear the configuration:

   `wipeconfig`

   Respond `yes` to the confirmation prompt.

   The node reboots and the boot menu is displayed again.

6. At the boot menu, select option **5** to boot the system into Maintenance mode.

   Respond `yes` to the confirmation prompt.

Verifying MetroCluster health before site upgrade

You must verify the health and connectivity of the MetroCluster configuration prior to performing the upgrade.

Steps

1. Verify the operation of the MetroCluster configuration in ONTAP:

   a. Check whether the nodes are multipathed:
   `node run -node` *`node-name`* `sysconfig -a`

      You should issue this command for each node in the MetroCluster configuration.

   b. Verify that there are no broken disks in the configuration:
   `storage disk show -broken`

      You should issue this command on each node in the MetroCluster configuration.

   c. Check for any health alerts:

      `system health alert show`

      You should issue this command on each cluster.

   d. Verify the licenses on the clusters:

      `system license show`

      You should issue this command on each cluster.

   e. Verify the devices connected to the nodes:

      `network device-discovery show`

      You should issue this command on each cluster.

   f. Verify that the time zone and time is set correctly on both sites:

      `cluster date show`

You should issue this command on each cluster. You can use the `cluster date` commands to configure the time and time zone.

2. Confirm the operational mode of the MetroCluster configuration and perform a MetroCluster check.
   a. Confirm the MetroCluster configuration and that the operational mode is `normal`:
      `metrocluster show`
   b. Confirm that all expected nodes are shown:
      `metrocluster node show`
   c. Issue the following command:

      `metrocluster check run`

   d. Display the results of the MetroCluster check:

      `metrocluster check show`

3. Check the MetroCluster cabling with the Config Advisor tool.
   a. Download and run Config Advisor.

      NetApp Downloads: Config Advisor

   b. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

Gathering information before the upgrade

Before upgrading, you must gather information for each of the nodes, and, if necessary, adjust the network broadcast domains, remove any VLANs and interface groups, and gather encryption information.

Steps

1. Record the physical cabling for each node, labelling cables as needed to allow correct cabling of the new nodes.
2. Gather interconnect, port and LIF information for each node.

   You should gather the output of the following commands for each node:

   - `metrocluster interconnect show`
   - `metrocluster configuration-settings connection show`
   - `network interface show -role cluster,node-mgmt`
   - `network port show -node node_name -type physical`
   - `network port vlan show -node` *`node-name`*
   - `network port ifgrp show -node` *`node_name`* `-instance`
   - `network port broadcast-domain show`
   - `network port reachability show -detail`
   - `network ipspace show`
   - `volume show`

◦ `storage aggregate show`
◦ `system node run -node` *`node-name`* `sysconfig -a`
◦ `vserver fcp initiator show`
◦ `storage disk show`
◦ `metrocluster configuration-settings interface show`

3. Gather the UUIDs for the site_B (the site whose platforms are currently being upgraded):

   `metrocluster node show -fields node-cluster-uuid, node-uuid`

   These values must be configured accurately on the new site_B controller modules to ensure a successful upgrade. Copy the values to a file so that you can copy them into the proper commands later in the upgrade process.

   The following example shows the command output with the UUIDs:

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid
  (metrocluster node show)
dr-group-id cluster     node   node-uuid
node-cluster-uuid
----------- --------- -------- ------------------------------------
------------------------------
1           cluster_A node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_A node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098908039
1           cluster_B node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098c9e55d
1           cluster_B node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098c9e55d
4 entries were displayed.
cluster_B::*
```

   It is recommended that you record the UUIDs into a table similar to the following.

Cluster or node	UUID
cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039

node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
node_A_2	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

4. If the MetroCluster nodes are in a SAN configuration, collect the relevant information.

   You should gather the output of the following commands:

   - `fcp adapter show -instance`
   - `fcp interface show -instance`
   - `iscsi interface show`
   - `ucadmin show`

5. If the root volume is encrypted, collect and save the passphrase used for key-manager:

   `security key-manager backup show`

6. If the MetroCluster nodes are using encryption for volumes or aggregates, copy information about the keys and passphrases.

   For additional information, see Backing up onboard key management information manually.

   a. If Onboard Key Manager is configured:
      `security key-manager onboard show-backup`

      You will need the passphrase later in the upgrade procedure.

   b. If enterprise key management (KMIP) is configured, issue the following commands:

      `security key-manager external show -instance` `security key-manager key query`

7. Gather the system IDs of the existing nodes:

   `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

   The following output shows the reassigned drives.

```
::> metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster     node     node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ----------- -------- ------------- -------------------
------------------- ---------------------
1           cluster_A node_A_1   537403324     537403323
537403321           537403322
1           cluster_A node_A_2   537403323     537403324
537403322           537403321
1           cluster_B node_B_1   537403322     537403321
537403323           537403324
1           cluster_B node_B_2   537403321     537403322
537403324           537403323
4 entries were displayed.
```

Removing Mediator or Tiebreaker monitoring

Before the upgrading the platforms, you must remove monitoring if the MetroCluster configuration is monitored with the Tiebreaker or Mediator utility.

Steps

1. Collect the output for the following command:

   `storage iscsi-initiator show`

2. Remove the existing MetroCluster configuration from Tiebreaker, Mediator, or other software that can initiate switchover.

If you are using…	Use this procedure…
Tiebreaker	Removing MetroCluster Configurations in the *MetroCluster Tiebreaker Installation and Configuration Guide*
Mediator	Issue the following command from the ONTAP prompt: `metrocluster configuration-settings mediator remove`
Third-party applications	Refer to the product documentation.

Sending a custom AutoSupport message prior to maintenance

Before performing the maintenance, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster.
2. Invoke an AutoSupport message indicating the start of the maintenance:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   The `maintenance-window-in-hours` parameter specifies the length of the maintenance window, with a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Repeat these steps on the partner site.

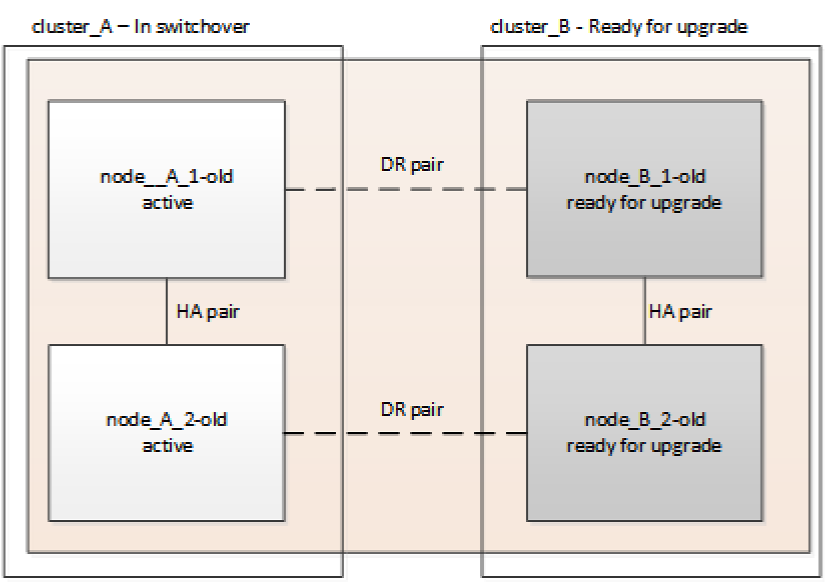
Switching over the MetroCluster configuration

You must switch over the configuration to site_A so that the platforms on site_B can be upgraded.

About this task

This task must be performed on site_A.

After completing this task, cluster_A is active and serving data for both sites. cluster_B is inactive, and ready to begin the upgrade process.



Steps

1. Switch over the MetroCluster configuration to site_A so that site_B's nodes can be upgraded:
   a. Issue the following command on cluster_A:

      ```
      metrocluster switchover -controller-replacement true
      ```

      The operation can take several minutes to complete.

   b. Monitor the switchover operation:

      ```
      metrocluster operation show
      ```

   c. After the operation is complete, confirm that the nodes are in switchover state:

      ```
      metrocluster show
      ```

   d. Check the status of the MetroCluster nodes:

      ```
      metrocluster node show
      ```

      Automatic healing of aggregates after negotiated switchover is disabled during controller upgrade.

Removing interface configurations and uninstalling the old controllers

You must move data LIFs to a common port, remove VLANs and interface groups on the old controllers and then physically uninstall the controllers.

About this task

- These steps are performed on the old controllers (node_B_1-old, node_B_2-old).
- See the information you gathered in Mapping ports from the old nodes to the new nodes.

Steps

1. Boot the old nodes and log in to the nodes:

   ```
   boot_ontap
   ```

2. Assign the home port of all data LIFs on the old controller to a common port that is the same on both the old and new controller modules.
   a. Display the LIFs:

      ```
      network interface show
      ```

      All data LIFS including SAN and NAS will be admin up and operationally down since those are up at switchover site (cluster_A).

   b. Review the output to find a common physical network port that is the same on both the old and new controllers that is not used as a cluster port.

      For example, e0d is a physical port on old controllers and is also present on new controllers. e0d is not used as a cluster port or otherwise on the new controllers.

      For port usage for platform models, see the NetApp Hardware Universe

c. Modify all data LIFS to use the common port as the home port:
`network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

In the following example, this is "e0d".

For example:

```
network interface modify -vserver vs0 -lif datalif1 -home-port e0d
```

3. Remove any VLAN ports using cluster ports as member ports and ifgrps using cluster ports as member ports.

a. Delete VLAN ports:
`network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

For example:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Remove physical ports from the interface groups:

`network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

For example:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

c. Remove VLAN and interface group ports from broadcast domain::

`network port broadcast-domain remove-ports -ipspace` *`ipspace`* `-broadcast -domain` *`broadcast-domain-name`* `-ports` *`nodename:portname,nodename:portname`*`,..`

d. Modify interface group ports to use other physical ports as member as needed.:

`ifgrp add-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`port-id`*

4. Halt the nodes to the LOADER prompt:

`halt -inhibit-takeover true`

5. Connect to the serial console of the old controllers (node_B_1-old and node_B_2-old) at site_B and verify it is displaying the LOADER prompt.

6. Gather the bootarg values:

`printenv`

7. Disconnect the storage and network connections on node_B_1-old and node_B_2-old and label the cables so they can be reconnected to the new nodes.

8. Disconnect the power cables from node_B_1-old and node_B_2-old.
9. Remove the node_B_1-old and node_B_2-old controllers from the rack.

Updating the switch RCFs to accommodate the new platforms

You must update the switches to a configuration that supports the new platform models.

About this task

You perform this task at the site containing the controllers that are currently being upgraded. In the examples shown in this procedure we are upgrading site_B first.

The switches at site_A will be upgraded when the controllers on site_A are upgraded.

Steps

1. Prepare the IP switches for the application of the new RCF files.

   Follow the steps in the section for your switch vendor from the *MetroCluster IP Installation and Configuration Guide*.

   MetroCluster IP installation and configuration

   - Resetting the Broadcom IP switch to factory defaults
   - Resetting the Cisco IP switch to factory defaults

2. Download and install the RCF files.

   Follow the steps in the section for your switch vendor from the MetroCluster IP installation and configuration.

   - Downloading and installing the Broadcom RCF files
   - Downloading and installing the Cisco IP RCF files

Configuring the new controllers

You must rack and install the controllers, perform required setup in Maintenance mode, and then boot the controllers, and verify the LIF configuration on the controllers.

Setting up the new controllers

You must rack and cable the new controllers.

Steps

1. Plan out the positioning of the new controller modules and storage shelves as needed.

   The rack space depends on the platform model of the controller modules, the switch types, and the number of storage shelves in your configuration.

2. Properly ground yourself.
3. Install the controller modules in the rack or cabinet.

   AFF and FAS Documentation Center

4. Cable the controllers to the IP switches as described in the *MetroCluster IP Installation and Configuration Guide*.

   MetroCluster IP installation and configuration

   ◦ Cabling the IP switches

5. Power up the new nodes and boot them to Maintenance mode.

Restoring the HBA configuration

Depending on the presence and configuration of HBA cards in the controller module, you need to configure them correctly for your site's usage.

Steps

1. In Maintenance mode configure the settings for any HBAs in the system:

   a. Check the current settings of the ports:

      `ucadmin show`

   b. Update the port settings as needed.

If you have this type of HBA and desired mode…	Use this command…
CNA FC	`ucadmin modify -m fc -t initiator` *`adapter-name`*
CNA Ethernet	`ucadmin modify -mode cna` *`adapter-name`*
FC target	`fcadmin config -t target` *`adapter-name`*
FC initiator	`fcadmin config -t initiator` *`adapter-name`*

2. Exit Maintenance mode:

   `halt`

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

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

   `boot_ontap maint`

4. Verify the changes you made:

If you have this type of HBA…	Use this command…
CNA	`ucadmin show`

FC	`fcadmin show`

Setting the HA state on the new controllers and chassis

You must verify the HA state of the controllers and chassis, and, if necessary, update the state to match your system configuration.

Steps

1. In Maintenance mode, display the HA state of the controller module and chassis:

   `ha-config show`

   The HA state for all components should be "mccip".

2. If the displayed system state of the controller or chassis is not correct, set the HA state:

   `ha-config modify controller mccip`

   `ha-config modify chassis mccip`

Setting the MetroCluster IP bootarg variables

Certain MetroCluster IP bootarg values must be configured on the new controller modules. The values must match those configured on the old controller modules.

About this task

In this task, you will use the UUIDs and system IDs identified earlier in the upgrade procedure in Gathering information before the upgrade.

Steps

1. If the nodes being upgraded are AFF A400, FAS8300, or FAS8700 models, set the following bootargs at the LOADER prompt:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address,vlan-id`*

   > If the interfaces are using the default VLANs, the vlan-id is not necessary.

   The following commands set the values for node_B_1-new using VLAN 120 for the first network and VLAN 130 for the second network:

   ```
   setenv bootarg.mcc.port_a_ip_config
   172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120
   setenv bootarg.mcc.port_b_ip_config
   172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
   ```

The following commands set the values for node_B_2-new using VLAN 120 for the first network and VLAN 130 for the second network:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13,120
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13,130
```

The following example shows the commands for node_B_1-new when the default VLAN is used:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

The following example shows the commands for node_B_2-new when the default VLAN is used:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

2. If the nodes being upgraded are not systems listed in the previous step, at the LOADER prompt for each of the surviving nodes, set the following bootargs with local_IP/mask:

   `setenv bootarg.mcc.port_a_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address`*

   `setenv bootarg.mcc.port_b_ip_config` *`local-IP-address/local-IP-mask,0,HA-partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address`*

   The following commands set the values for node_B_1-new:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12
setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

   The following commands set the values for node_B_2-new:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.11/23,0,172.17.26.10,172.17.26.12,172.17.26.13
setenv bootarg.mcc.port_b_ip_config
172.17.27.11/23,0,172.17.27.10,172.17.27.12,172.17.27.13
```

3. At the new nodes' LOADER prompt, set the UUIDs:

   `setenv bootarg.mgwd.partner_cluster_uuid` *`partner-cluster-UUID`*

   `setenv bootarg.mgwd.cluster_uuid` *`local-cluster-UUID`*

   `setenv bootarg.mcc.pri_partner_uuid` *`DR-partner-node-UUID`*

   `setenv bootarg.mcc.aux_partner_uuid` *`DR-aux-partner-node-UUID`*

   `setenv bootarg.mcc_iscsi.node_uuid` *`local-node-UUID`*

   a. Set the UUIDs on node_B_1-new.

      The following example shows the commands for setting the UUIDs on node_B_1-new:

      ```
      setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
      setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
      00a098ca379f
      setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
      00a098908039
      ```

   b. Set the UUIDs on node_B_2-new:

      The following example shows the commands for setting the UUIDs on node_B_2-new:

      ```
      setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039
      setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
      00a098ca379f
      setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-
      00a098c9e55d
      setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-
      00a098908c35
      ```

4. If the original systems were configured for ADP, at each of the replacement nodes' LOADER prompt, enable ADP:

   `setenv bootarg.mcc.adp_enabled true`

5. Set the following variables:

   `setenv bootarg.mcc.local_config_id original-sys-id`

   `setenv bootarg.mcc.dr_partner dr-partner-sys-id`

   > The `setenv bootarg.mcc.local_config_id` variable must be set to the sys-id of the **original** controller module, node_B_1-old.

   a. Set the variables on node_B_1-new.

      The following example shows the commands for setting the values on node_B_1-new:

      ```
      setenv bootarg.mcc.local_config_id 537403322
      setenv bootarg.mcc.dr_partner 537403324
      ```

   b. Set the variables on node_B_2-new.

      The following example shows the commands for setting the values on node_B_2-new:

      ```
      setenv bootarg.mcc.local_config_id 537403321
      setenv bootarg.mcc.dr_partner 537403323
      ```

6. If using encryption with external key manager, set the required bootargs:

   `setenv bootarg.kmip.init.ipaddr`

   `setenv bootarg.kmip.kmip.init.netmask`

   `setenv bootarg.kmip.kmip.init.gateway`

   `setenv bootarg.kmip.kmip.init.interface`

Reassigning root aggregate disks

Reassign the root aggregate disks to the new controller module, using the sysids gathered earlier.

About this task

These steps are performed in Maintenance mode.

Steps

1. Boot the system to Maintenance mode:

   `boot_ontap maint`

2. Display the disks on node_B_1-new from the Maintenance mode prompt:

   `disk show -a`

   The command output shows the system ID of the new controller module (1574774970). However, the root aggregate disks are still owned by the old system ID (537403322). This example does not show drives owned by other nodes in the MetroCluster configuration.

```
*> disk show -a
Local System ID: 1574774970
DISK                  OWNER                 POOL   SERIAL NUMBER   HOME
DR HOME
------------          ---------             -----  -------------
-------------         -------------
prod3-rk18:9.126L44   node_B_1-old(537403322)  Pool1  PZHYN0MD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:9.126L49   node_B_1-old(537403322)  Pool1  PPG3J5HA
node_B_1-old(537403322)  node_B_1-old(537403322)
prod4-rk18:8.126L21   node_B_1-old(537403322)  Pool1  PZHTDSZD
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L2    node_B_1-old(537403322)  Pool0  S0M1J2CF
node_B_1-old(537403322)  node_B_1-old(537403322)
prod2-rk18:8.126L3    node_B_1-old(537403322)  Pool0  S0M0CQM5
node_B_1-old(537403322)  node_B_1-old(537403322)
prod1-rk18:9.126L27   node_B_1-old(537403322)  Pool0  S0M1PSDW
node_B_1-old(537403322)  node_B_1-old(537403322)
.
.
.
```

3. Reassign the root aggregate disks on the drive shelves to the new controllers.

If you are using ADP…	Then use this command…
Yes	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`* `-r` *`dr-partner-sysid`*
No	`disk reassign -s` *`old-sysid`* `-d` *`new-sysid`*

4. Reassign the root aggregate disks on the drive shelves to the new controllers:

   `disk reassign -s old-sysid -d new-sysid`

   The following example shows reassignment of drives in a non-ADP configuration:

```
*> disk reassign -s 537403322 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537403322.
Do you want to continue (y/n)? y
```

5. Verify that the disks of the root aggregate are properly reassigned old-remove:

```
disk show
```

```
storage aggr status
```

```
*> disk show
Local System ID: 537097247

  DISK                    OWNER                    POOL   SERIAL NUMBER
HOME                     DR HOME
------------             -------------            -----  -------------
-------------            -------------
prod03-rk18:8.126L18 node_B_1-new(537097247)  Pool1  PZHYN0MD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:9.126L49 node_B_1-new(537097247)  Pool1  PPG3J5HA
node_B_1-new(537097247)   node_B_1-new(537097247)
prod04-rk18:8.126L21 node_B_1-new(537097247)  Pool1  PZHTDSZD
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:8.126L2  node_B_1-new(537097247)  Pool0  S0M1J2CF
node_B_1-new(537097247)   node_B_1-new(537097247)
prod02-rk18:9.126L29 node_B_1-new(537097247)  Pool0  S0M0CQM5
node_B_1-new(537097247)   node_B_1-new(537097247)
prod01-rk18:8.126L1  node_B_1-new(537097247)  Pool0  S0M1PSDW
node_B_1-new(537097247)   node_B_1-new(537097247)
::>
::> aggr status
           Aggr          State           Status               Options
aggr0_node_B_1           online          raid_dp, aggr        root,
nosnap=on,
                                         mirrored
mirror_resync_priority=high(fixed)
                                         fast zeroed
                                         64-bit
```

Booting up the new controllers

You must boot the new controllers, taking care to ensure that the bootarg variables are correct and, if needed, perform the encryption recovery steps.

Steps

1. Halt the new nodes:

   `halt`

2. If external key manager is configured, set the related bootargs:

   `setenv bootarg.kmip.init.ipaddr` *`ip-address`*

   `setenv bootarg.kmip.init.netmask` *`netmask`*

   `setenv bootarg.kmip.init.gateway` *`gateway-address`* `setenv bootarg.kmip.init.interface interface-id`

3. Check if the partner-sysid is the current:

   `printenv partner-sysid`

   If the partner-sysid is not correct, set it:

   `setenv partner-sysid partner-sysID`

4. Display the ONTAP boot menu:

   `boot_ontap menu`

5. If root encryption is used, issue the boot menu command for your key management configuration.

If you are using…	Issue this command at the boot menu prompt…
Onboard key management	`recover_onboard_keymanager`
External key management	`recover_external_keymanager`

6. From the boot menu, select “(6) Update flash from backup config”.

   Option 6 will reboot the node twice before completing.

   Respond `y` to the system id change prompts. Wait for the second reboot messages:

```
Successfully restored env file from boot media...

Rebooting to load the restored env file...
```

7. On LOADER, double-check the bootarg values and update the values as needed.

   Use the steps in Setting the MetroCluster IP bootarg variables.

8. Double-check that the partner-sysid is the correct:

   `printenv partner-sysid`

   If the partner-sysid is not correct, set it:

   `setenv partner-sysid partner-sysID`

9. If root encryption is used, again issue the boot menu command for your key management configuration.

If you are using…	Issue this command at the boot menu prompt…
Onboard key management	`recover_onboard_keymanager`

External key management	`recover_external_keymanager`

You may need to issue the `recover_xxxxxxxx_keymanager` command and option 6 at the boot menu prompt multiple times until the nodes fully boot.

10. Wait for the replaced nodes to boot up.

    If either node is in takeover mode, perform a giveback using the `storage failover giveback` command.

11. If encryption is used, restore the keys using the correct command for your key management configuration.

If you are using…	Use this command…
Onboard key management	`security key-manager onboard sync` For more information, see Restoring onboard key management encryption keys.
External key management	`security key-manager external restore -vserver` *`SVM`* `-node` *`node`* `-key-server` *`host_name|IP_address:port`* `-key-id key_id -key-tag key_tag` *`node-name`* For more information, see Restoring external key management encryption keys.

12. Verify that all ports are in a broadcast domain:

    a. View the broadcast domains:

       `network port broadcast-domain show`

    b. Add any ports to a broadcast domain as needed.

       Adding or removing ports from a broadcast domain

    c. Recreate VLANs and interface groups as needed.

       VLAN and interface group membership might be different than that of the old node.

       Creating a VLAN

       Combining physical ports to create interface groups

Verifying and restoring LIF configuration

Verify that LIFs are hosted on appropriate nodes and ports as mapped out at the beginning of the upgrade procedure.

About this tsak

* This task is performed on site_B.
* See the port mapping plan you created in Mapping ports from the old nodes to the new nodes.

Steps

1. Verify that LIFs are hosted on the appropriate node and ports prior to switchback.
   a. Change to the advanced privilege level:

      ```
      set -privilege advanced
      ```

   b. Override the port configuration to ensure proper LIF placement:

      ```
      vserver config override -command "network interface modify -vserver
      vserver_name -home-port active_port_after_upgrade -lif lif_name -home-node
      new_node_name"
      ```

      When entering the network interface modify command within the `vserver config override` command, you cannot use the tab autocomplete feature. You can create the network `interface modify` using autocomplete and then enclose it in the `vserver config override` command.

   c. Return to the admin privilege level:

      ```
      set -privilege admin
      ```

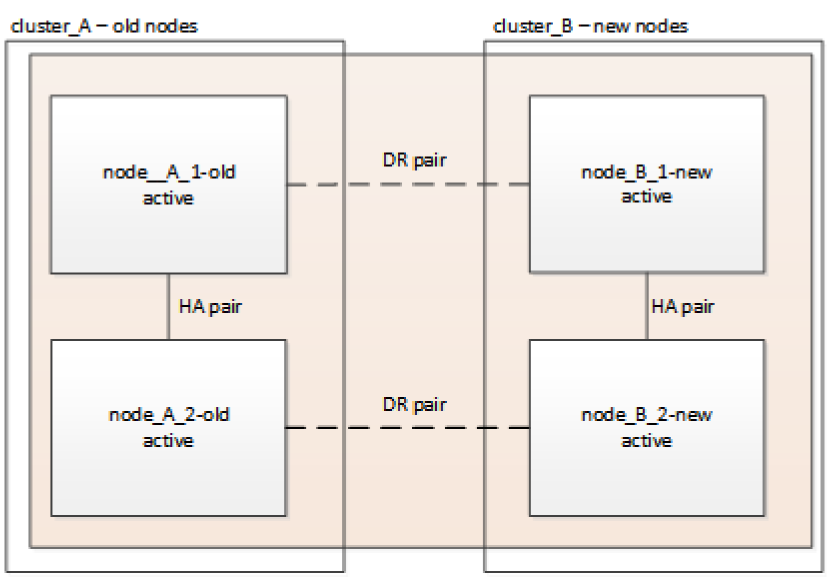
2. Revert the interfaces to their home node:

   ```
   network interface revert * -vserver vserver-name
   ```

   Perform this step on all SVMs as required.

Switching back the MetroCluster configuration

In this task, you will perform the switchback operation, and the MetroCluster configuration returns to normal operation. The nodes on site_A are still awaiting upgrade.



Steps

1. Issue the `metrocluster node show` command on site_B and check the output.
   a. Verify that the new nodes are represented correctly.
   b. Verify that the new nodes are in "Waiting for switchback state."
2. Perform the healing and switchback by running the required commands from any node in the active cluster (the cluster that is not undergoing upgrade).
   a. Heal the data aggregates:
      `metrocluster heal aggregates`
   b. Heal the root aggregates:

      `metrocluster heal root`

   c. Switchback the cluster:

      `metrocluster switchback`

3. Check the progress of the switchback operation:

   `metrocluster show`

   The switchback operation is still in progress when the output displays `waiting-for-switchback`:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

   The switchback operation is complete when the output displays normal:

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

   If a switchback takes a long time to finish, you can check on the status of in-progress baselines by using the `metrocluster config-replication resync-status show` command. This command is at the advanced privilege level.

Checking the health of the MetroCluster configuration

After upgrading the controller modules you must verify the health of the MetroCluster configuration.

About this task

This task can be performed on any node in the MetroCluster configuration.

Steps

1. Verify the operation of the MetroCluster configuration:

   a. Confirm the MetroCluster configuration and that the operational mode is normal:
   `metrocluster show`

   b. Perform a MetroCluster check:
   `metrocluster check run`

   c. Display the results of the MetroCluster check:

   ```
   metrocluster check show
   ```

2. Verify the MetroCluster connectivity and status.

   a. Check the MetroCluster IP connections:

   ```
   storage iscsi-initiator show
   ```

   b. Check that the nodes are operating:

   ```
   metrocluster node show
   ```

   c. Check that the MetroCluster IP interfaces are up:

   ```
   metrocluster configuration-settings interface show
   ```

   d. Check that local failover is enabled:

   ```
   storage failover show
   ```

Upgrading the nodes on cluster_A

You must repeat the upgrade tasks on cluster_A.

Steps

1. Repeat the steps to upgrade the nodes on cluster_A, beginning with Preparing for the upgrade.

   As you perform the tasks, all example references to the clusters and nodes are reversed. For example, when the example is given to switchover from cluster_A, you will switchover from cluster_B.

Restoring Tiebreaker or Mediator monitoring

After completing the upgrade of the MetroCluster configuration, you can resume monitoring with the Tiebreaker or Mediator utility.

Steps

1. Restore monitoring if necessary, using the procedure for your configuration.

If you are using…	Use this procedure
Tiebreaker	Adding MetroCluster configurations in the *MetroCluster Tiebreaker Installation and Configuration Guide*
Mediator	Configuring the ONTAP Mediator service from a MetroCluster IP configuration in the *MetroCluster IP Installation and Configuration Guide*
Third-party applications	Refer to the product documentation.

Sending a custom AutoSupport message after maintenance

After completing the upgrade, you should send an AutoSupport message indicating the end of maintenance, so automatic case creation can resume.

Steps

1. To resume automatic support case generation, send an Autosupport message to indicate that the maintenance is complete.
   a. Issue the following command:
      `system node autosupport invoke -node * -type all -message MAINT=end`
   b. Repeat the command on the partner cluster.

Refreshing a four-node MetroCluster FC configuration

You can upgrade the controllers and storage in a four-node MetroCluster configuration by expanding the configuration to become an eight-node configuration and then removing the old disaster recovery (DR) group.

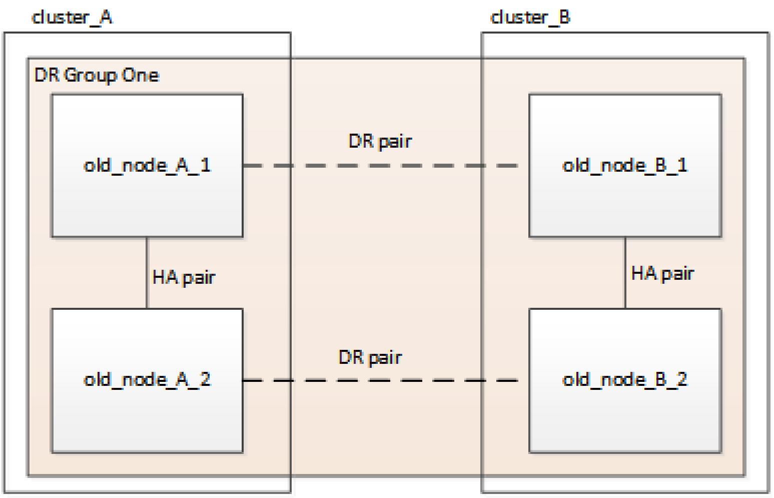
About this task

References to "old nodes" mean the nodes that you intend to replace.

Steps

1. Gather information from the old nodes.

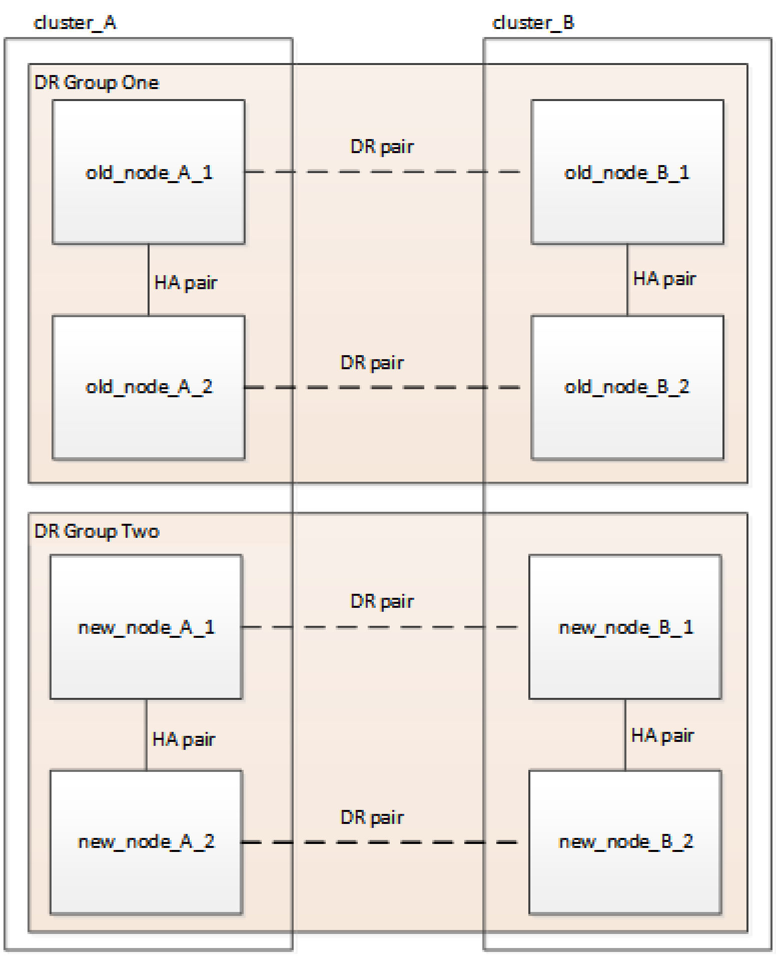
   At this stage, the four-node configuration appears as shown in the following image:



2. Perform all of the steps in the four-node expansion procedure for your MetroCluster type.

   Expanding a four-node MetroCluster FC configuration to an eight-node configuration

   When the expansion procedure is complete, the configuration appears as shown in the following image:



3. Move the CRS volumes.

   Perform the steps in Moving a metadata volume in MetroCluster configurations.

4. Move the data from the old nodes to new nodes using the following three procedures from the *Controller Hardware Upgrade Express Guide*.

   Other platform procedures: Controller Hardware Upgrade Express Guide

   a. Perform all the steps in Creating an aggregate and moving volumes to the new nodes.

      You might choose to mirror the aggregate when or after it is created.

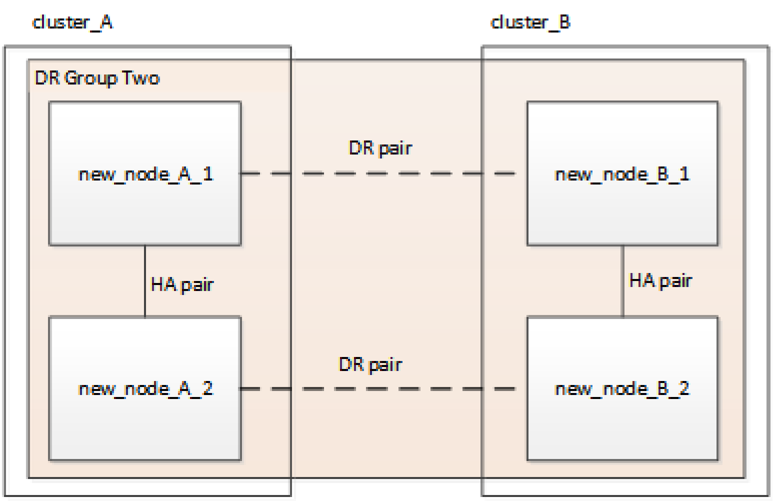
   b. Perform all the steps in Moving non-SAN data LIFs and cluster management LIFs to the new nodes.

   c. Perform all the steps in Deleting SAN LIFs from the original nodes.

5. Follow the steps in the procedure for removing the old DR group.

   Removing a Disaster Recovery group

   After you have removed the old DR group (DR group one), the configuration appears as shown in the following image:



Refreshing a four-node MetroCluster IP configuration (ONTAP 9.8 and later)

Starting with ONTAP 9.8, you can upgrade the controllers and storage in a four-node MetroCluster IP configuration by expanding the configuration to become a temporary eight-node configuration and then removing the old disaster recovery (DR) group.

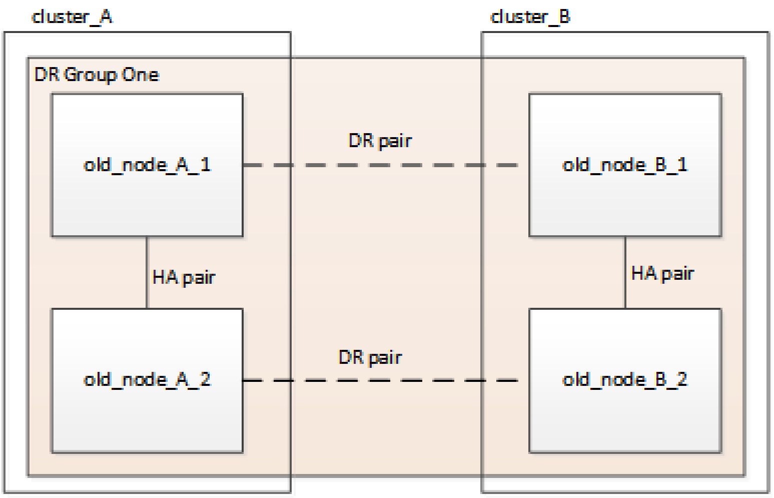
About this task

- This procedure is supported on systems running ONTAP 9.8 and later.
- If you are upgrading the IP switches, they should be upgraded before to performing this refresh procedure.
- References to "old nodes" mean the nodes that you intend to replace.
- This procedure is not supported on AFF A320 systems configured with Broadcom BES-53248 switches.

Steps

1. Gather information from the old nodes.

At this stage, the four-node configuration appears as shown in the following image:



2. To prevent automatic support case generation, send an Autosupport message to indicate the upgrade is underway.
   a. Issue the following command:
      `system node autosupport invoke -node * -type all -message "MAINT=10h Upgrading old-model to new-model"`

      The following example specifies a 10 hour maintenance window. You might want to allow additional time depending on your plan.

      If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

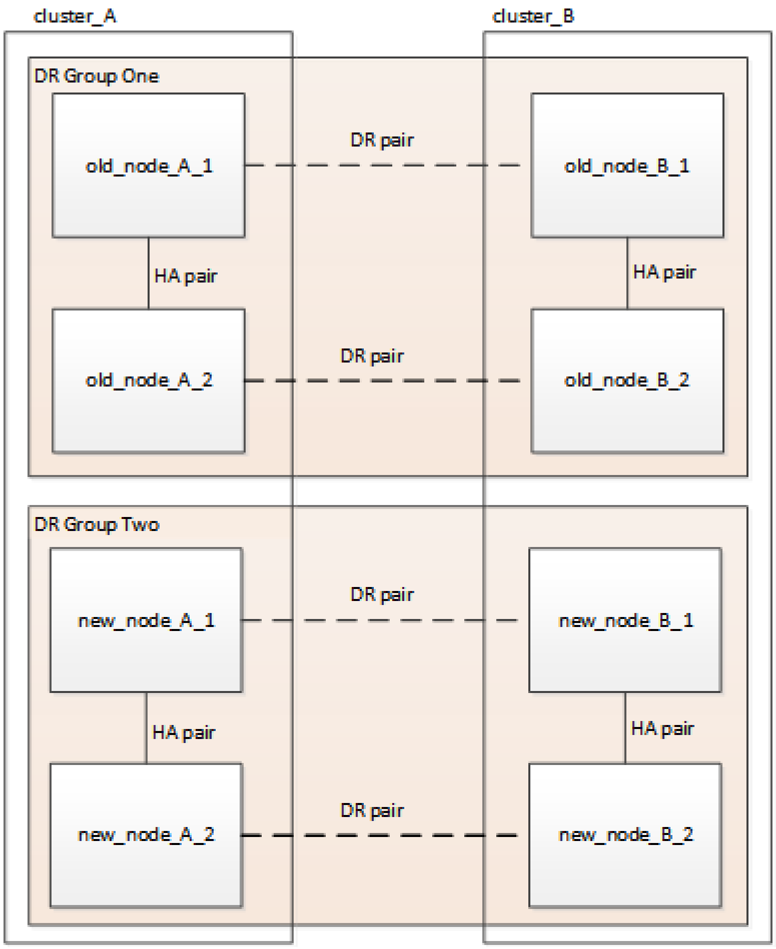
      ```
      system node autosupport invoke -node * -type all -message MAINT=end
      ```

   b. Repeat the command on the partner cluster.
3. Remove the existing MetroCluster configuration from Tiebreaker, Mediator, or other software that can initiate switchover.

If you are using…	Use this procedure…
Tiebreaker	Removing MetroCluster Configurations in the *MetroCluster Tiebreaker Installation and Configuration Guide*
Mediator	Issue the following command from the ONTAP prompt: `metrocluster configuration-settings mediator remove`
Third-party applications	Refer to the product documentation.

4. Perform all of the steps in Expanding a four-node MetroCluster IP configuration to an eight-node configuration to add the new nodes and storage to the configuration.

When the expansion procedure is complete, the configuration appears as shown in the following image:



5. Move the CRS volumes.

   Perform the steps in Moving a metadata volume in MetroCluster configurations.

6. Move the data from the old nodes to new nodes using the following procedures from the *Controller Hardware Upgrade Express Guide*.

   Other platform procedures: Controller Hardware Upgrade Express Guide

   a. Perform all the steps in Creating an aggregate and moving volumes to the new nodes.

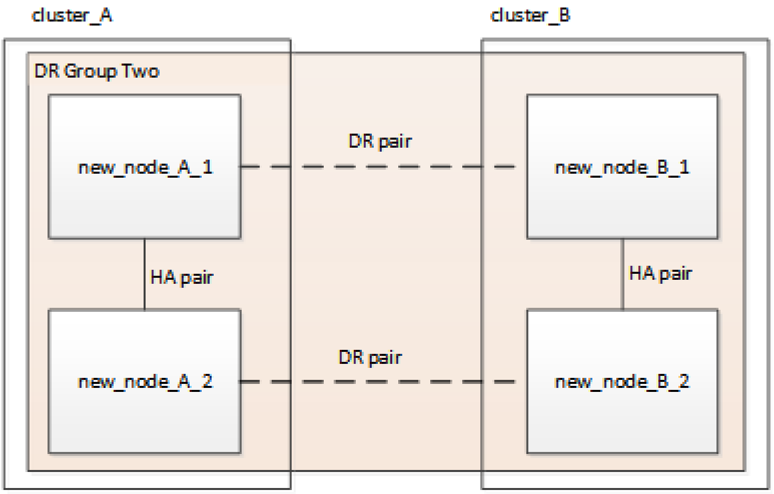
      You might choose to mirror the aggregate when or after it is created.

   b. Perform all the steps in Moving non-SAN data LIFs and cluster management LIFs to the new nodes.

7. Follow the steps in the procedure for removing the old DR group.

   Removing a Disaster Recovery group

   After you have removed the old DR group (DR group one), the configuration appears as shown in the following image:



8. Confirm the operational mode of the MetroCluster configuration and perform a MetroCluster check.
   a. Confirm the MetroCluster configuration and that the operational mode is normal:

      ```
      metrocluster show
      ```

   b. Confirm that all expected nodes are shown:

      ```
      metrocluster node show
      ```

   c. Issue the following command:

      ```
      metrocluster check run
      ```

   d. Display the results of the MetroCluster check:

      ```
      metrocluster check show
      ```

9. Restore monitoring if necessary, using the procedure for your configuration.

If you are using…	Use this procedure
Tiebreaker	Adding MetroCluster configurations in the *MetroCluster Tiebreaker Installation and Configuration Guide*
Mediator	Configuring the ONTAP Mediator service from a MetroCluster IP configuration in the *MetroCluster IP Installation and Configuration Guide*
Third-party applications	Refer to the product documentation.

10. To resume automatic support case generation, send an Autosupport message to indicate that the maintenance is complete.
    a. Issue the following command:

       ```
       system node autosupport invoke -node * -type all -message MAINT=end
       ```

b. Repeat the command on the partner cluster.

Expanding a two-node MetroCluster FC configuration to a four-node configuration

Expanding a two-node MetroCluster FC configuration to a four-node MetroCluster FC configuration involves adding a controller to each cluster to form an HA pair at each MetroCluster site, and then refreshing the MetroCluster FC configuration.

Before you begin

- The nodes must be running ONTAP 9 or later in a MetroCluster FC configuration.

  This procedure is not supported on earlier versions of ONTAP or in MetroCluster IP configurations.

- If the platforms in your two-node configuration are not supported in ONTAP 9.2 and you plan to upgrade to platforms supported in ONTAP 9.2 *and* expand to a four-node cluster, you must upgrade the platforms in the two-node configuration *before* expanding the MetroCluster FC configuration.
- The existing MetroCluster FC configuration must be healthy.
- The equipment you are adding must be supported and meet all of the requirements described in the *Fabric-attached MetroCluster Installation and Configuration Guide* or the *Stretch Installation and Configuration Guide*.

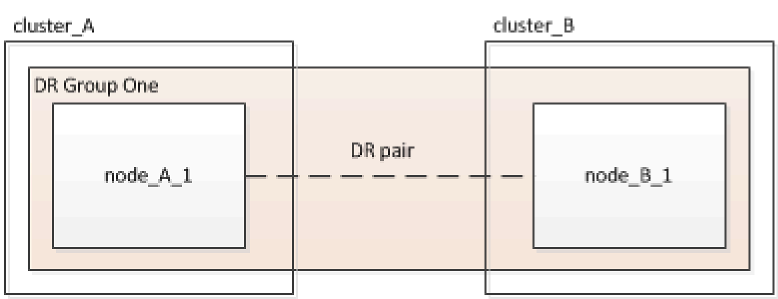
  Fabric-attached MetroCluster installation and configuration

  Stretch MetroCluster installation and configuration

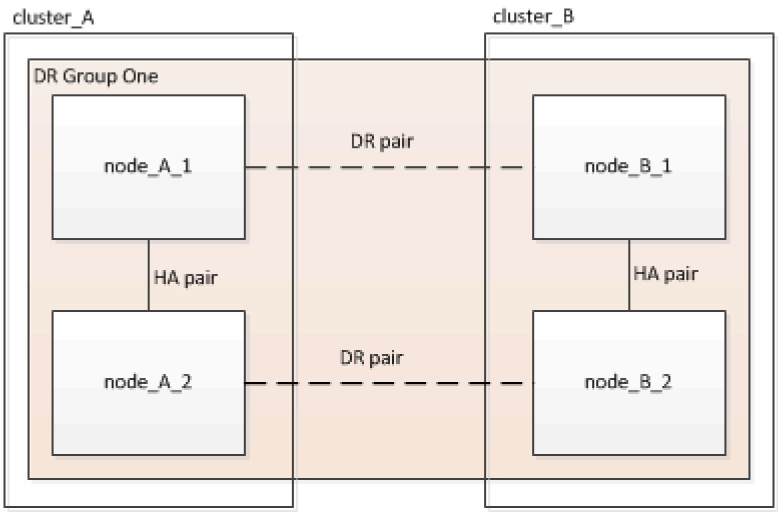
- You must have available FC switch ports to accommodate the new controllers and any new bridges.
- You need the admin password and access to an FTP or SCP server.

About this task

- This procedure applies only to MetroCluster FC configurations.
- This procedure is disruptive and takes approximately four hours to complete.
- Before performing this procedure, the MetroCluster FC configuration consists of two single-node clusters:



  After completing this procedure, the MetroCluster FC configuration consists of two HA pairs, one at each site:



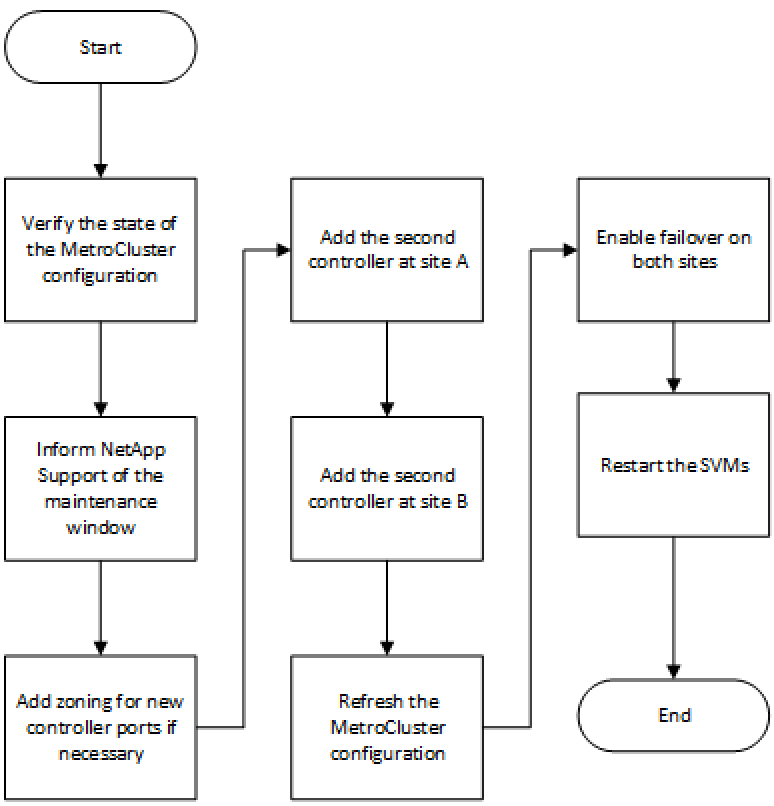
* Both sites must be expanded equally.

  A MetroCluster configuration cannot consist of an uneven number of nodes.

* This procedure can take over an hour per site, with additional time for tasks such as initializing the disks and netbooting the new nodes.

  The time to initialize the disks depends on the size of the disks.

* This procedure uses the following workflow:



Verifying the state of the MetroCluster configuration

You should identify the existing controllers and confirm the disaster recovery (DR) relationships between them, that the controllers are in normal mode, and that the aggregates are mirrored.

Steps

1. Display the details of the nodes in the MetroCluster configuration from any node in the configuration:

   `metrocluster node show -fields node,dr-partner,dr-partner-systemid`

   The following output shows that this MetroCluster configuration has a single DR group and one node in each cluster.

   ```
   cluster_A::> metrocluster node show -fields node,dr-partner,dr-partner-
   systemid

   dr-group-id  cluster         node            dr-partner      dr-partner-
   systemid
   -----------  -------------   -------         ----------
   -------------------
   1            cluster_A       controller_A_1  controller_B_1  536946192
   1            cluster_B       controller_B_1  controller_A_1  536946165
   2 entries were displayed.
   ```

2. Display the state of the MetroCluster configuration:

   `metrocluster show`

   The following output shows that the existing nodes in the MetroCluster configuration are in normal mode:

   ```
   cluster_A::> metrocluster show

   Configuration: two-node-fabric

   Cluster                        Entry Name             State
   ------------------------------ ----------------------
   ---------------------
   Local: cluster_A               Configuration State    configured
                                  Mode                   normal
                                  AUSO Failure Domain    auso-on-cluster-
   disaster
   Remote: controller_B_1_siteB
                                  Configuration State    configured
                                  Mode                   normal
                                  AUSO Failure Domain    auso-on-cluster-
   disaster
   ```

3. Check the state of the aggregates on each node in the MetroCluster configuration:

```
storage aggregate show
```

The following output shows that the aggregates on cluster_A are online and mirrored:

```
cluster_A::> storage aggregate show


Aggregate                Size     Available Used%  State   #Vols  Nodes
RAID Status
---------                -------- --------- -----  ------- ------
---------------- ------------
aggr0_controller_A_1_0   1.38TB   68.63GB   95%    online    1
controller_A_1   raid_dp,mirrored
controller_A_1_aggr1     4.15TB   4.14TB    0%     online    2
controller_A_1   raid_dp,mirrored
controller_A_1_aggr2     4.15TB   4.14TB    0%     online    1
controller_A_1   raid_dp,mirrored
3 entries were displayed.

cluster_A::>
```

Sending a custom AutoSupport message before adding nodes to the MetroCluster configuration

You should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster at Site_A.
2. Invoke an AutoSupport message indicating the start of the maintenance:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   The `maintenance-window-in-hours` parameter specifies the length of the maintenance window and can be a maximum of 72 hours. If you complete the maintenance before the time has elapsed, you can issue the following command to indicate that the maintenance period has ended:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Repeat this step on the partner site.

Zoning for the new controller ports when adding a controller module in a fabric-attached MetroCluster configuration

The FC switch zoning must accommodate the new controller connections. If you used the NetApp-supplied reference configuration files (RCFs) to configure your switches, the zoning is preconfigured and you do not need to make any changes.

If you manually configured your FC switches, you must ensure that the zoning is correct for the initiator connections from the new controller modules. See the sections on zoning in the *Fabric-attached MetroCluster Installation and Configuration Guide*.

[Fabric-attached MetroCluster installation and configuration]

Adding a new controller module to each cluster

You must add a new controller module to each site, creating an HA pair in each site. This is a multistep process involving both hardware and software changes that must be performed in the proper order at each site.

About this task

- The new controller module must be received from NetApp as part of the upgrade kit.

  You should verify that PCIe cards in the new controller module are compatible and supported by the new controller module.

  [NetApp Hardware Universe]

- Your system must have an empty slot available for the new controller module when upgrading to a single-chassis HA pair (an HA pair in which both controller modules reside in the same chassis).

  > This configuration is not supported on all systems. Platforms with single chassis configurations that are supported in ONTAP 9 are AFF A300, FAS8200, FAS8300, AFF A400, AFF80xx, FAS8020, FAS8060, FAS8080, and FAS9000.

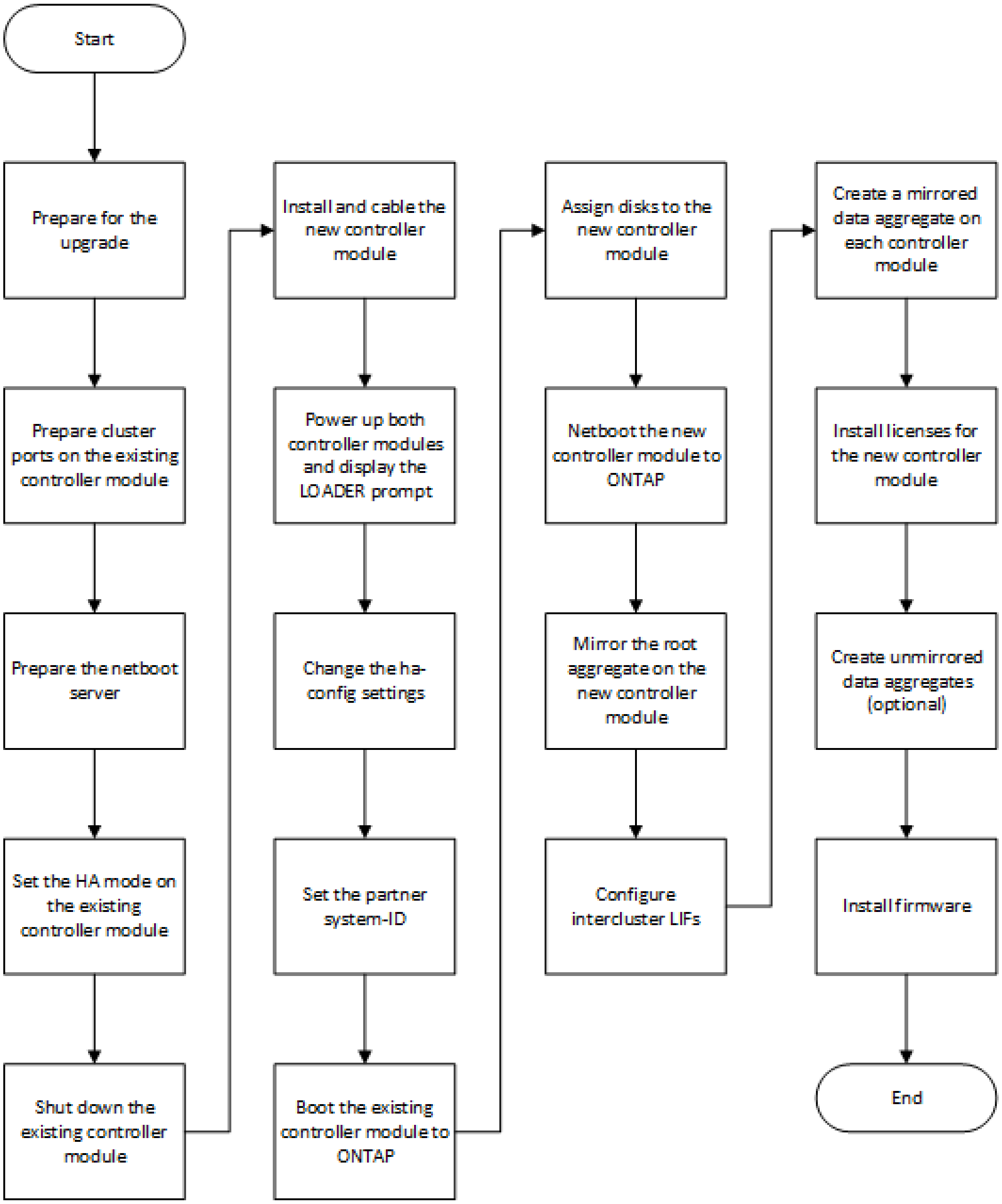
- You must have rack space and cables for the new controller module when upgrading to a dual-chassis HA pair (an HA pair in which the controller modules reside in separate chassis).

  > This configuration is not supported on all systems.

- You must connect each controller module to the management network through its e0a port or, if your system has one, you can connect to the e0M port as the management port.
- These tasks must be repeated at each site.
- The preexisting controller modules are referred to as the *existing* controller modules.

  The examples in this procedure have the console prompt `existing_ctlr>`.

- The controller modules that are being added are referred to as the *new* controller modules; the examples in this procedure have the console prompt `new_ctlr>`.
- This task uses the following workflow:



Preparing for the upgrade

Before upgrading to an HA pair, you must verify that your system meets all requirements and that you have all of the necessary information.

Steps

1. You need to identify unassigned disks or spare disks that you can assign to the new controller module.

   Physical Storage Management Guide

   Disk and aggregate management

2. Based on the results of the previous step, perform either of the following:

If the result showed…	Then…

Not enough spare disks available for the new controller module on a system without root-data partitioning	Contact technical support for more information.

Other results	Complete the following substeps:
	
	a. Determine where the aggregates for the existing node are located:
	
	`storage aggregate show`
	
	b. If disk ownership automatic assignment is on, turn it off:
	
	`storage disk option modify -node` *`node_name`* `-autoassign off`
	
	c. Remove ownership on disks that do not have aggregates on them:
	
	`storage disk removeowner` *`disk_name`*
	
	d. Repeat the previous step for as many disks as you need for the new node.

3. Verify that you have cables ready for the following connections:
   - Cluster connections

     If you are creating a two-node switchless cluster, you require two cables to connect the controller modules. Otherwise, you require a minimum of four cables, two for each controller module connection to the cluster-network switch. Other systems (like the 80xx series) have defaults of either four or six cluster connections.

   - HA interconnect connections, if the system is in a dual-chassis HA pair
4. Verify that you have a serial port console available for the controller modules.
5. Verify that your environment meets the site and system requirements.

   NetApp Hardware Universe

6. Gather all of the IP addresses and other network parameters for the new controller module.

Clearing the configuration on a controller module

Before using a new controller module in the MetroCluster configuration, you must clear the existing configuration.

Steps

1. If necessary, halt the node to display the LOADER prompt:

   ```
   halt
   ```

2. At the LOADER prompt, set the environmental variables to default values:

```
set-defaults
```

3. Save the environment:

```
saveenv
```

4. At the LOADER prompt, launch the boot menu:

```
boot_ontap menu
```

5. At the boot menu prompt, clear the configuration:

```
wipeconfig
```

Respond `yes` to the confirmation prompt.

The node reboots and the boot menu is displayed again.

6. At the boot menu, select option **5** to boot the system into Maintenance mode.

Respond `yes` to the confirmation prompt.

Preparing cluster ports on an existing controller module

Before installing a new controller module, you must configure cluster ports on the existing controller module so that the cluster ports can provide cluster communication with the new controller module.

About this task

If you are creating a two-node switchless cluster (with no cluster network switches), you must enable the switchless cluster networking mode.

For detailed information about port, LIF, and network configuration in ONTAP, see the Network Management Guide.

Steps

1. Determine which ports should be used as the node's cluster ports.

   For a list of the default port roles for your platform, see the Hardware Universe

   The *Installation and Setup Instructions* for your platform on the NetApp Support Site contains information about the ports for cluster network connections.

2. For each cluster port, identify the port roles:

   ```
   network port show
   ```

   In the following example, ports "e0a", "e0b", "e0c", and "e0d" must be changed to cluster ports:

```
cluster_A::> network port show

Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Default      Default          up    1500   auto/10000  healthy
e0b       Default      Default          up    1500   auto/10000  healthy
e0c       Default      Default          up    1500   auto/10000  healthy
e0d       Default      Default          up    1500   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10     -
e0j       Default      Default          down  1500   auto/10     -
e0k       Default      Default          down  1500   auto/10     -
e0l       Default      Default          down  1500   auto/10     -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

3. For any data LIF that is using a cluster port as the home-port or current-port, modify the LIF to use a data port as its home-port:

   `network interface modify`

   The following example changes the home port of a data LIF to a data port:

   ```
   cluster1::> network interface modify -lif datalif1 -vserver vs1 -home
   -port e1b
   ```

4. For each LIF that you modified, revert the LIF to its new home port:

   `network interface revert`

   The following example reverts the LIF "datalif1" to its new home port "e1b":

   ```
   cluster1::> network interface revert -lif datalif1 -vserver vs1
   ```

5. Remove any VLAN ports using cluster ports as member ports and ifgrps using cluster ports as member ports.

   a. Delete VLAN ports:
      `network port vlan delete -node` *`node-name`* `-vlan-name` *`portid-vlandid`*

For example:

```
network port vlan delete -node node1 -vlan-name e1c-80
```

b. Remove physical ports from the interface groups:

`network port ifgrp remove-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`portid`*

For example:

```
network port ifgrp remove-port -node node1 -ifgrp a1a -port e0d
```

c. Remove VLAN and interface group ports from broadcast domain::

`network port broadcast-domain remove-ports -ipspace` *`ipspace`* `-broadcast -domain` *`broadcast-domain-name`* `-ports` *`nodename:portname,nodename:portname`*`,..`

d. Modify interface group ports to use other physical ports as member as needed.:
`ifgrp add-port -node` *`node-name`* `-ifgrp` *`interface-group-name`* `-port` *`port-id`*

6. Verify that the port roles have changed:

`network port show`

The following example shows that ports "e0a", "e0b", "e0c", and "e0d" are now cluster ports:

```
Node: controller_A_1
Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link  MTU    Admin/Oper  Status
--------- ------------ ---------------- ----  ----   -----------
--------
e0M       Default      mgmt_bd_1500     up    1500   auto/1000   healthy
e0a       Cluster      Cluster          up    9000   auto/10000  healthy
e0b       Cluster      Cluster          up    9000   auto/10000  healthy
e0c       Cluster      Cluster          up    9000   auto/10000  healthy
e0d       Cluster      Cluster          up    9000   auto/10000  healthy
e0i       Default      Default          down  1500   auto/10 -
e0j       Default      Default          down  1500   auto/10 -
e0k       Default      Default          down  1500   auto/10 -
e0l       Default      Default          down  1500   auto/10 -
e2a       Default      Default          up    1500   auto/10000  healthy
e2b       Default      Default          up    1500   auto/10000  healthy
e4a       Default      Default          up    1500   auto/10000  healthy
e4b       Default      Default          up    1500   auto/10000  healthy
13 entries were displayed.
```

7. Add the ports to the cluster broadcast domain:

   `broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster -ports` *`port-id, port-id, port-id…`*

   For example:

   ```
   broadcast-domain add-ports -ipspace Cluster -broadcast-domain Cluster
   -ports cluster1-01:e0a
   ```

8. If your system is part of a switched cluster, create cluster LIFs on the cluster ports: `network interface create`

   The following example creates a cluster LIF on one of the node's cluster ports. The `-auto` parameter configures the LIF to use a link-local IP address.

   ```
   cluster1::> network interface create -vserver Cluster -lif clus1 -role
   cluster -home-node node0 -home-port e1a -auto true
   ```

9. If you are creating a two-node switchless cluster, enable the switchless cluster networking mode:
   a. Change to the advanced privilege level from either node:

      `set -privilege advanced`

      You can respond `y` when prompted whether you want to continue into advanced mode. The advanced mode prompt appears (`*>`).

   b. Enable the switchless cluster networking mode:

      `network options switchless-cluster modify -enabled true`

   c. Return to the admin privilege level:

      `set -privilege admin`

> Cluster interface creation for the existing node in a two-node switchless cluster system is completed after cluster setup is completed through a netboot on the new controller module.

Preparing the netboot server to download the image

When you are ready to prepare the netboot server, you must download the correct ONTAP netboot image from the NetApp Support Site to the netboot server and note the IP address.

About this task

- You must be able to access an HTTP server from the system before and after adding the new controller module.

- You must have access to the NetApp Support Site to download the necessary system files for your platform and your version of ONTAP.

  NetApp Support Site

- Both controller modules in the HA pair must run the same version of ONTAP.

Steps

1. Download the appropriate ONTAP software from the software download section of the NetApp Support Site and store the `<ontap_version>_image.tgz` file on a web-accessible directory.

   The `<ontap_version>_image.tgz` file is used for performing a netboot of your system.

2. Change to the web-accessible directory and verify that the files you need are available.

For…	Then…

FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 series systems	Extract the contents of the <ontap_version>_image.tgz file to the target directory:
	
	`tar -zxvf <ontap_version>_image.tgz`
	
	If you are extracting the contents on Windows, use 7-Zip or WinRAR to extract the netboot image.
	
	Your directory listing should contain a netboot folder with a kernel file:
	
	`netboot/kernel`

All other systems	Your directory listing should contain the following file: `<ontap_version>_image.tgz` There is no need to extract the file contents.

3. Determine the IP address of the existing controller module.

   This address is referred to later in this procedure as *`ip-address-of-existing controller`*.

4. Ping *`ip-address-of-existing controller`* to verify that the IP address is reachable.

Setting the HA mode on the existing controller module

You must use the storage failover modify command to set the mode on the existing controller module. The mode value is enabled later, after you reboot the controller module.

Steps

1. Set the mode to HA:

   `storage failover modify -mode ha -node` *`existing_node_name`*

Shutting down the existing controller module

You must perform a clean shutdown of the existing controller module to verify that all of the data has been written to disk. You must also disconnect the power supplies.

About this task

> You must perform a clean system shutdown before replacing the system components to avoid losing unwritten data in the NVRAM or NVMEM.

Steps

1. Halt the node from the existing controller module prompt:

   `halt local -inhibit-takeover true`

   If you are prompted to continue the halt procedure, enter `y` when prompted, and then wait until the system stops at the LOADER prompt.

   In an 80xx system, the NVRAM LED is located on the controller module to the right of the network ports, marked with a battery symbol.

   This LED blinks if there is unwritten data in the NVRAM. If this LED is flashing amber after you enter the halt command, you need to reboot your system and try halting it again.

2. If you are not already grounded, properly ground yourself.
3. Turn off the power supplies and disconnect the power, using the correct method for your system and power-supply type:

If your system uses…	Then…
AC power supplies	Unplug the power cords from the power source, and then remove the power cords.
DC power supplies	Remove the power at the DC source, and then remove the DC wires, if necessary.

Installing and cabling the new controller module

You must physically install the new controller module in the chassis, and then cable it.

Steps

1. If you have an I/O expansion module (IOXM) in your system and are creating a single-chassis HA pair, you must uncable and remove the IOXM.

   You can then use the empty bay for the new controller module. However, the new configuration will not have the extra I/O provided by the IOXM.

2. Physically install the new controller module and, if necessary, install additional fans:

If you are adding a controller module…	Then perform these steps…
To an empty bay to create a single-chassis HA pair and the system belongs to one of the following platforms:	a. Remove the blank plate in the rear of the chassis that covers the empty bay that will contain the new controller module. b. Gently push the controller module halfway into the chassis. To prevent the controller module from automatically booting, do not fully seat it in the chassis until later in this procedure.
In a separate chassis from its HA partner to create a dual-chassis HA pair when the existing configuration is in a controller-IOX module configuration. • FAS8200 • 80xx	Install the new system in the rack or system cabinet.

3. Cable the cluster network connections, as necessary:

   a. Identify the ports on the controller module for the cluster connections.

      AFF A320 systems: Installation and setup

      AFF A220/FAS2700 Systems Installation and Setup Instructions

      AFF A800 Systems Installation and Setup Instructions

      AFF A300 Systems Installation and Setup Instructions

      FAS8200 Systems Installation and Setup Instructions

   b. If you are configuring a switched cluster, identify the ports that you will use on the cluster network switches.

      See the *Clustered Data ONTAP Switch Setup Guide for Cisco Switches*, *NetApp 10G Cluster-Mode Switch Installation Guide* or *NetApp 1G Cluster-Mode Switch Installation Guide*, depending on what switches you are using.

   c. Connect cables to the cluster ports:

If the cluster is…	Then…
A two-node switchless cluster	Directly connect the cluster ports on the existing controller module to the corresponding cluster ports on the new controller module.

A switched cluster	Connect the cluster ports on each controller to the ports on the cluster network switches identified in substep b.

Cabling the new controller module’s FC-VI and HBA ports to the FC switches

The new controller module’s FC-VI ports and HBAs (host bus adapters) must be cabled to the site FC switches.

Steps

1. Cable the FC-VI ports and HBA ports, using the table for your configuration and switch model.
   - Port assignments for FC switches when using ONTAP 9.1 and later
   - Port assignments for FC switches when using ONTAP 9.0
   - Port assignments for systems using two initiator ports

Cabling the new controller module’s cluster peering connections

You must cable the new controller module to the cluster peering network so that it has connectivity with the cluster on the partner site.

About this task

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.

Steps

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

Powering up both controller modules and displaying the LOADER prompt

You power up the existing controller module and the new controller module to display the LOADER prompt.

Steps

Power up the controller modules and interrupt the boot process, using the steps for your configuration:

If the controller modules are…	Then…

In the same chassis	a. Verify that the new controller module is **not** fully inserted into the bay. The existing controller module should be fully inserted into the bay because it was never removed from the chassis, but the new controller module should not be. b. Connect the power and turn on the power supplies so that the existing controller module receives power. c. Interrupt the boot process on the existing controller module by pressing Ctrl-C. d. Push the new controller module firmly into the bay. When fully seated, the new controller module receives power and automatically boots. e. Interrupt the boot process by pressing Ctrl-C. f. Tighten the thumbscrew on the cam handle, if present. g. Install the cable management device, if present. h. Bind the cables to the cable management device with the hook and loop strap.
In separate chassis	a. Turn on the power supplies on the existing controller module. b. Interrupt the boot process by pressing Ctrl-C. c. Repeat these steps for the new controller module

Each controller module should display the LOADER prompt (`LOADER>`, `LOADER-A>`, or `LOADER-B>`).

> If there is no LOADER prompt, record the error message and contact technical support. If the system displays the boot menu, reboot and attempt to interrupt the boot process again.

Changing the ha-config setting on the existing and new controller modules

When you expand a MetroCluster configuration, you must update the ha-config setting of the existing controller module and the new controller module. You must also determine the system ID of the new controller module.

About this task

This task is performed in Maintenance mode on both the existing and new controller modules.

Steps

1. Change the ha-config setting of the existing controller module:
   a. Display the ha-config setting of the existing controller module and chassis:

      ```
      ha-config show
      ```

      The ha-config setting is “mcc-2n” for all components because the controller module was in a two-node MetroCluster configuration.

b. Change the ha-config setting of the existing controller module to “mcc”:
   `ha-config modify controller mcc`
c. Change the ha-config setting of the existing chassis to “mcc”:

   `ha-config modify chassis mcc`

d. Retrieve the system ID for the existing controller module:

   `sysconfig`

   Note the system ID. You need it when you set the partner ID on the new controller module.

e. Exit Maintenance mode to return to the LOADER prompt:

   `halt`

2. Change the ha-config setting and retrieve the system ID of the new controller module:
   a. If the new controller module is not already in Maintenance mode, boot it to Maintenance mode:

      `boot_ontap maint`

   b. Change the ha-config setting of the new controller module to “mcc”:

      `ha-config modify controller mcc`

   c. Change the ha-config setting of the new chassis to mcc:

      `ha-config modify chassis mcc`

   d. Retrieve the system ID for the new controller module:

      `sysconfig`

      Note the system ID. You need it when you set the partner ID and assign disks to the new controller module.

   e. Exit Maintenance mode to return to the LOADER prompt:

      `halt`

Setting the partner system ID for both controller modules

You must set the partner system ID on both controller modules so that they can form an HA pair.

About this task

This task is performed with both controller modules at the LOADER prompt.

Steps

1. On the existing controller module, set the partner system ID to that of the new controller module:

   `setenv partner-sysid` *`sysID_of_new_controller`*

2. On the new controller module, set the partner system ID to that of the existing controller module:

   `setenv partner-sysid` *`sysID_of_existing_controller`*

Booting the existing controller module

You must boot the existing controller module to ONTAP.

Steps

1. At the LOADER prompt, boot the existing controller module to ONTAP:

   `boot_ontap`

Assigning disks to the new controller module

Before you complete the configuration of the new controller module through netboot, you must assign disks to it.

About this task

You must have made sure that there are enough spares, unassigned disks, or assigned disks that are not part of an existing aggregate.

Preparing for the upgrade

These steps are performed on the existing controller module.

Steps

1. Assign the root disk to the new controller module:

   `storage disk assign -disk` *`disk_name`* `-sysid` *`new_controller_sysID`* `-force true`

   If your platform model uses the Advanced Drive Partitioning (ADP) feature, you must include the -root true parameter:

   `storage disk assign -disk` *`disk_name`* `-root true -sysid` *`new_controller_sysID`* `-force true`

2. Assign the remaining required disks to the new controller module by entering the following command for each disk:

   `storage disk assign -disk` *`disk_name`* `-sysid` *`new_controller_sysID`* `-force true`

3. Verify that the disk assignments are correct:

   `storage disk show -partitionownership*`

   > Ensure that you have assigned all disks that you intend to assign to the new node.

Netbooting and setting up ONTAP on the new controller module

You must perform a specific sequence of steps to netboot and install the ONTAP operating system on the new controller module when adding controller modules to an existing MetroCluster configuration.

About this task

- This task starts at the LOADER prompt of the new controller module.
- This task includes initializing disks.

  The amount of time you need to initialize the disks depends on the size of the disks.

- The system automatically assigns two disks to the new controller module.

  Disk and aggregate management

Steps

1. At the LOADER prompt, configure the IP address of the new controller module based on DHCP availability:

If DHCP is…	Then enter the following command…
Available	**`ifconfig e0M -auto`**
Not available	`ifconfig e0M -addr=`*`filer_addr`*` -mask=`*`netmask`*` -gw=`*`gateway`*` -dns=`*`dns_addr`*` -domain=`*`dns_domain`* `filer_addr` is the IP address of the storage system. `netmask` is the network mask of the storage system. `gateway` is the gateway for the storage system. `dns_addr` is the IP address of a name server on your network. `dns_domain` is the Domain Name System (DNS) domain name. If you use this optional parameter, you do not need a fully qualified domain name in the netboot server URL; you need only the server's host name. Other parameters might be necessary for your interface. For details, use the `help ifconfig` command at the LOADER prompt.

2. At the LOADER prompt, netboot the new node:

For…	Issue this command…
FAS2200, FAS2500, FAS3200, FAS6200, FAS/AFF8000 series systems	`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`
All other systems	`netboot http://web_server_ip/path_to_web-accessible_directory/<ontap_version>_image.tgz`

The *path_to_the_web-accessible_directory* is the location of the downloaded `<ontap_version>_image.tgz` file.

3. Select the **Install new software first** option from the displayed menu.

   This menu option downloads and installs the new ONTAP image to the boot device.

   - You should enter **y** when prompted with the message that this procedure is not supported for nondisruptive upgrade on an HA pair.
   - You should enter **y** when warned that this process replaces the existing ONTAP software with new software.
   - You should enter the path as follows when prompted for the URL of the image.tgz file:

     `http://path_to_the_web-accessible_directory/image.tgz`

4. Enter **y** when prompted regarding nondisruptive upgrade or replacement of the software.
5. Enter the path to the image.tgz file when prompted for the URL of the package.

```
What is the URL for the package? `http://path_to_web-
accessible_directory/image.tgz`
```

6. Enter **n** to skip the backup recovery when prompted to restore the backup configuration.

```
****************************************************************
*              Restore Backup Configuration                    *
*  This procedure only applies to storage controllers that     *
*  are configured as an HA pair.                               *
*                                                              *
*  Choose Yes to restore the "varfs" backup configuration      *
*  from the SSH server.  Refer to the Boot Device Replacement  *
*  guide for more details.                                     *
*  Choose No to skip the backup recovery and return to the     *
*  boot menu.                                                  *
****************************************************************

Do you want to restore the backup configuration
now? {y|n} `n`
```

7. Enter **y** when prompted to reboot now.

```
The node must be rebooted to start using the newly installed software.
Do you want to
reboot now? {y|n} `y`
```

8. If necessary, select the option to **Clean configuration and initialize all disks** after the node has booted.

   Because you are configuring a new controller module and the new controller module's disks are empty, you can respond **y** when the system warns you that this will erase all disks.

   > The amount of time needed to initialize disks depends on the size of your disks and configuration.

9. After the disks are initialized and the Cluster Setup wizard starts, set up the node:

   Enter the node management LIF information on the console.

10. Log in to the node, and enter the `cluster setup` and then enter `join` when prompted to join the cluster.

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

11. Respond to the remaining prompts as appropriate for your site.

    The Software Setup Guide for your version of ONTAP contains additional details.

12. If the system is in a two-node switchless cluster configuration, create the cluster interfaces on the existing node using the network interface create command to create cluster LIFs on the cluster ports.

    The following is an example command for creating a cluster LIF on one of the node's cluster ports. The

-auto parameter configures the LIF to use a link-local IP address.

```
cluster_A::> network interface create -vserver Cluster -lif clus1 -role
cluster -home-node node_A_1 -home-port e1a -auto true
```

13. After setup is complete, verify that the node is healthy and eligible to participate in the cluster:

    `cluster show`

    The following example shows a cluster after the second node (cluster1-02) has been joined to it:

```
cluster_A::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node_A_1              true    true
node_A_2              true    true
```

    You can access the Cluster Setup wizard to change any of the values you entered for the admin storage virtual machine (SVM) or node SVM by using the cluster setup command.

14. Confirm that you have four ports configured as cluster interconnects:

    `network port show`

    The following example shows output for two controller modules in cluster_A:

```
cluster_A::> network port show
                                                              Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU     Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **e0a       Cluster      Cluster          up       9000
auto/1000
       e0b       Cluster      Cluster          up       9000
auto/1000**
       e0c       Default      Default          up       1500  auto/1000
       e0d       Default      Default          up       1500  auto/1000
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

Mirroring the root aggregate on the new controller

You must mirror the root aggregate to provide data protection when you are adding a controller to a MetroCluster configuration.

This task must be performed on the new controller module.

1. Mirror the root aggregate:

   `storage aggregate mirror` *`aggr_name`*

   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.

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.

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.

   The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                             Speed
(Mbps)
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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

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.

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

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

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`*

   The following example assigns ports "e0e" and "e0f" to the failover group "intercluster01" on the system SVM "cluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verify that the failover group was created:

   `network interface failover-groups show`

   For complete command syntax, see the man page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

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

ONTAP version	Command
9.6 and later	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover -group failover_group`
9.5 and earlier	`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.

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

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-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 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster -failover`

In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

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 -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

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.

   The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                              Speed
(Mbps)
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:

In ONTAP 9.6 and later:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 and earlier:
`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.

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

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

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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:

In ONTAP 9.6 and later:
`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

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

```
cluster01::> network interface show -service-policy default-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
```

Creating a mirrored data aggregate on each node

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

About this task

- You should know what drives 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.
- Drives 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.

  In systems using ADP, aggregates are created using partitions in which each drive is partitioned in to P1, P2 and P3 partitions.

- 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:

   `storage aggregate create -mirror true`

   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 that are to be added to the aggregate
◦ Number of drives to include

> 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 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.

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`*

Installing licenses for the new controller module

You must add licenses for the new controller module for any ONTAP services that require standard (node-locked) licenses. For features with standard licenses, each node in the cluster must have its own key for the feature.

For detailed information about licensing, see the knowledgebase article 3013749: Data ONTAP 8.2 Licensing Overview and References on the NetApp Support Site and the *System Administration Reference*.

Steps

1. If necessary, obtain license keys for the new node on the NetApp Support Site in the My Support section under Software licenses.

   If the site does not have the license keys you need, contact your sales or support representative.

2. Issue the following command to install each license key:

```
system license add -license-code license_key
```

The *license_key* is 28 digits in length.

3. Repeat this step for each required standard (node-locked) license.

Creating unmirrored data aggregates

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

About this task

- 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.

> In MetroCluster IP configurations, remote unmirrored aggregates are not accessible after a switchover

> 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. Enable unmirrored aggregate deployment:

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment true
   ```

2. Verify that disk auto-assignment is disabled:

   ```
   disk option show
   ```

3. Install and cable the disk shelves that will contain the unmirrored aggregates.

   You can use the procedures in the *Installation and Setup* documentation for your platform and disk shelves.

   AFF and FAS Documentation Center

4. Manually assign all disks on the new shelf to the appropriate node:

   ```
   disk assign -disk disk-id -owner owner-node-name
   ```

5. Create the aggregate:

   ```
   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 must also ensure that you are only including drives on the unmirrored shelf to the aggregate.

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.

  The following command creates a unmirrored aggregate with 10 disks:

  ```
  controller_A_1::> storage aggregate create aggr1_controller_A_1
  -diskcount 10 -node controller_A_1
  [Job 15] Job is queued: Create aggr1_controller_A_1.
  [Job 15] The job is starting.
  [Job 15] Job succeeded: DONE
  ```

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

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

7. Disable unmirrored aggregate deployment:

   `metrocluster modify -enable-unmirrored-aggr-deployment false`

8. Verify that disk auto-assignment is enabled:

   `disk option show`

Related information

Disk and aggregate management

Installing the firmware after adding a controller module

After adding the controller module, you must install the latest firmware on the new controller module so that the controller module functions properly with ONTAP.

Steps

1. Download the most current version of firmware for your system and follow the instructions for downloading and installing the new firmware.

   NetApp Downloads: System Firmware and Diagnostics

Refreshing the MetroCluster configuration with new controllers

You must refresh the MetroCluster configuration when expanding it from a two-node configuration to a four-node configuration.

Steps

1. Refresh the MetroCluster configuration:

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

   b. Refresh the MetroCluster configuration:
      `metrocluster configure -refresh true -allow-with-one-aggregate true`

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

      ```
      controller_A_1::*> metrocluster configure -refresh true -allow-with
      -one-aggregate true

      [Job 726] Job succeeded: Configure is successful.
      ```

   c. Return to admin privilege mode:

      `set -privilege admin`

2. Verify the networking status on site A:

   `network port show`

   The following example shows the network port usage on a four-node MetroCluster configuration:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verify the MetroCluster configuration from both sites in the MetroCluster configuration.
   a. Verify the configuration from site A:

      `metrocluster show`

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

   b. Verify the configuration from site B:

      `metrocluster show`

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-cluster-
disaster
```

c. Verify that the DR relationships have been created correctly:

`metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-limit,automatic-uso,ha-partner,dr-partner`

```
metrocluster node show -fields dr-cluster,dr-auxiliary,node-object-
limit,automatic-uso,ha-partner,dr-partner
dr-group-id cluster     node    ha-partner dr-cluster  dr-partner
dr-auxiliary  node-object-limit automatic-uso
----------- ---------   ----    ---------- ----------  ----------
------------  ----------------- -------------
2           cluster_A   node_A_1 node_A_2    cluster_B  node_B_1
node_B_2      on                true
2           cluster_A   node_A_2 node_A_1    cluster_B  node_B_2
node_B_1      on                true
2           cluster_B   node_B_1 node_B_2    cluster_A  node_A_1
node_A_2      on                true
2           cluster_B   node_B_2 node_B_1    cluster_A  node_A_2
node_A_1      on                true
4 entries were displayed.
```

Enabling storage failover on both controller modules and enabling cluster HA

After adding new controller modules to the MetroCluster configuration, you must enable storage failover on both controller modules and separately enable cluster HA.

Before you begin

The MetroCluster configuration must have previously been refreshed using the `metrocluster configure -refresh true` command.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Enable storage failover:

   `storage failover modify -enabled true -node existing-node-name`

   The single command enables storage failover on both controller modules.

2. Verify that storage failover is enabled:

   `storage failover show`

   The output should be similar to the following:

   ```
   Node           Partner        Possible State Description
   -------------- -------------- -------- ----------------------
   old-ctlr        new-ctlr      true      Connected to new-ctlr
   new-ctlr        old-ctlr      true      Connected to old-ctlr
   2 entries were displayed.
   ```

3. Enable cluster HA:

   `cluster ha modify -configured true`

   Cluster high availability (HA) must be configured in a cluster if it contains only two nodes and it differs from the HA provided by storage failover.

Restarting the SVMs

After expanding the MetroCluster configuration, you must restart the SVMs.

Steps

1. Identify the SVMs that need to be restarted:

   `metrocluster vserver show`

   This command shows the SVMs on both MetroCluster clusters.

2. Restart the SVMs on the first cluster:

   a. Enter advanced privilege mode, pressing **`y`** when prompted:

      `set -privilege advanced`

   b. Restart the SVMs:

      `vserver start -vserver SVM_name -force true`

   c. Return to admin privilege mode:

      `set -privilege admin`

3. Repeat the previous step on the partner cluster.
4. Verify that the SVMs are in a healthy state:

```
metrocluster vserver show
```

Expanding a four-node MetroCluster FC configuration to an eight-node configuration

Expanding a four-node MetroCluster FC configuration to an eight-node MetroCluster FC configuration involves adding two controllers to each cluster to form a second HA pair at each MetroCluster site, and then running the MetroCluster FC configuration operation.

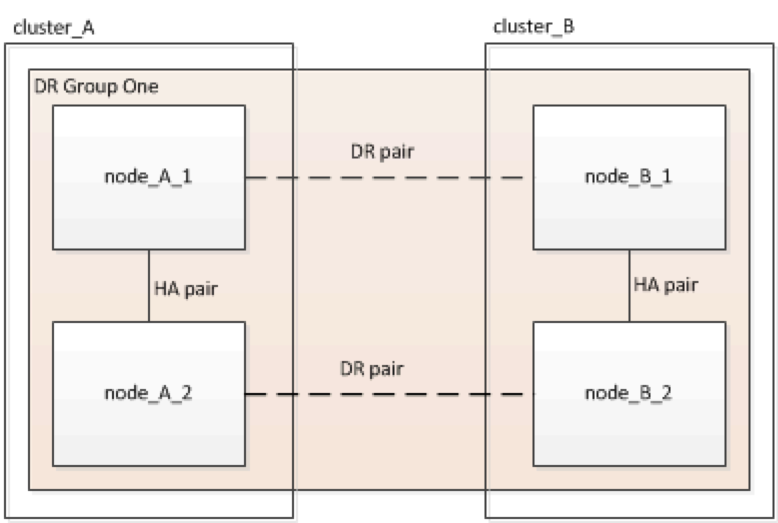
About this task

- The nodes must be running ONTAP 9 in a MetroCluster FC configuration.

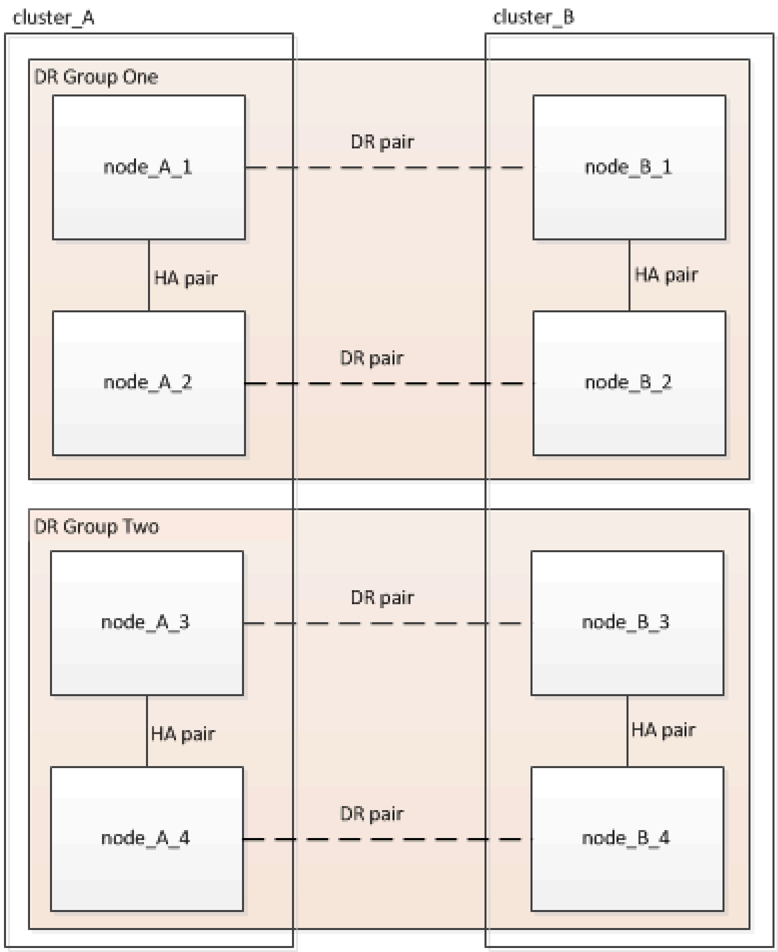
  This procedure is not supported on earlier versions of ONTAP or in MetroCluster IP configurations.

- The existing MetroCluster FC configuration must be healthy.
- The equipment you are adding must be supported and meet all the requirements described in Fabric-attached MetroCluster installation and configuration
- You must have available FC switch ports to accommodate the new controllers and any new bridges.
- You need the admin password and access to an FTP or SCP server.
- This procedure applies only to MetroCluster FC configurations.
- This procedure is nondisruptive and takes approximately one day to complete (excluding rack and stack) when disks are zeroed.

Before performing this procedure, the MetroCluster FC configuration consists of four nodes, with one HA pair at each site:



At the conclusion of this procedure, the MetroCluster FC configuration consists of two HA pairs at each site:



Both sites must be expanded equally. A MetroCluster FC configuration cannot consist of an uneven number of nodes.

Determining the new cabling layout

You must determine the cabling for the new controller modules and any new disk shelves to the existing FC switches.

About this task

This task must be performed at each MetroCluster site.

Steps

1. Use the *Fabric-attached MetroCluster Installation and Configuration Guide* and create a cabling layout for your switch type, using the port usage for an eight-node MetroCluster configuration.

   The FC switch port usage must match the usage described in the guide so that the Reference Configuration Files (RCFs) can be used.

   Fabric-attached MetroCluster installation and configuration

   > If your environment cannot be cabled in such a way that RCF files can be used, you must manually configure the system according to instructions found in the *Fabric-attached MetroCluster Installation and Configuration Guide*. Do not use this procedure if the cabling cannot use RCF files.

Racking the new equipment

You must rack the equipment for the new nodes.

Steps

1. Use the MetroCluster Installation and Configuration guide and rack the new storage systems, disk shelves, and FC-to-SAS bridges.

   Fabric-attached MetroCluster installation and configuration

Verifying the health of the MetroCluster configuration

You should check the health of the MetroCluster configuration to verify proper operation.

Steps

1. Check that the MetroCluster is configured and in normal mode on each cluster:

   `metrocluster show`

   ```
   cluster_A::> metrocluster show
   Cluster                   Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   ```

2. Check that mirroring is enabled on each node:

   `metrocluster node show`

   ```
   cluster_A::> metrocluster node show
   DR                           Configuration  DR
   Group Cluster Node           State          Mirroring Mode
   ----- ------- -------------- -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1       configured     enabled   normal
         cluster_B
                 node_B_1       configured     enabled   normal
   2 entries were displayed.
   ```

3. Check that the MetroCluster components are healthy:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

4. Check that there are no health alerts:

```
system health alert show
```

5. Simulate a switchover operation:

   a. From any node's prompt, change to the advanced privilege level:
   `set -privilege advanced`

   You need to respond with **y** when prompted to continue into advanced mode and see the advanced mode prompt (*>).

   b. Perform the switchover operation with the -simulate parameter:
   `metrocluster switchover -simulate`

   c. Return to the admin privilege level:
   `set -privilege admin`

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.

> ⓘ 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.

Sending a custom AutoSupport message prior to adding nodes to the MetroCluster configuration

You should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster at Site_A.
2. Invoke an AutoSupport message indicating the start of the maintenance:

   `system node autosupport invoke -node * -type all -message MAINT=`*`maintenance-window-in-hours`*

   The `maintenance-window-in-hours` parameter specifies the length of the maintenance window and can be a maximum of 72 hours. If the maintenance is completed before the time has elapsed, you can issue the following command to indicating that the maintenance period has ended:

   `system node autosupport invoke -node * -type all -message MAINT=end`

3. Repeat this step on the partner site.

Recabling and zoning a switch fabric for the new nodes

When adding nodes to the MetroCluster configuration, you must change the cabling and then run RCF files to redefine the zoning on the fabric.

About this task

This task must be performed on each switch fabric. It is done one fabric at a time.

Disconnecting the existing DR group from the fabric

You must disconnect the existing controller modules from the FC switches in the fabric.

About this task

This task must be performed at each MetroCluster site.

Steps

1. Disable the HBA ports that connect the existing controller modules to the switch fabric undergoing maintenance:

```
storage port disable -node node-name -port port-number
```

2. On the local FC switches, remove the cables from the ports for the existing controller module's HBA, FC-VI, and ATTO bridges.

   You should label the cables for easy identification when you re-cable them. Only the ISL ports should remain cabled.

Applying the RCF files and recabling the switches

You must apply the RCF files to reconfigure your zoning to accommodate the new nodes.

Steps

1. Locate the RCF files for your configuration.

   You must use the RCF files for an eight-node configuration and that match your switch model.

2. Apply the RCF files, following the directions on the download page, adjusting the ISL settings as needed.
3. Ensure that the switch configuration is saved.
4. Reboot the FC switches.
5. Cable both the pre-existing and the new FC-to-SAS bridges to the FC switches, using the cabling layout you created previously.

   The FC switch port usage must match the MetroCluster eight-node usage described in the *Fabric-attached MetroCluster Installation and Configuration Guide* so that the Reference Configuration Files (RCFs) can be used.

   Fabric-attached MetroCluster installation and configuration

   > ⓘ If your environment cannot be cabled in such a way that RCF files can be used then contact technical support. Do NOT use this procedure if the cabling cannot use RCF files.

6. Verify that the ports are online by using the correct command for your switch.

Switch vendor	Command
Brocade	switchshow
Cisco	show interface brief

7. Cable the FC-VI ports from the existing and new controllers, using the cabling layout you created previously.

   Fabric-attached MetroCluster installation and configuration

   The FC switch port usage must match the MetroCluster eight-node usage described in the *Fabric-attached MetroCluster Installation and Configuration Guide* so that the Reference Configuration Files (RCFs) can be used.

> If your environment cannot be cabled in such a way that RCF files can be used then contact technical support. Do NOT use this procedure if the cabling cannot use RCF files.

8. From the existing nodes, verify that the FC-VI ports are online:

   `metrocluster interconnect adapter show`

   `metrocluster interconnect mirror show`

9. Cable the HBA ports from the current and the new controllers.
10. On the existing controller modules, e-enable the ports connected to the switch fabric undergoing maintenance:

    `storage port enable -node` *`node-name`* `-port` *`port-ID`*

11. Start the new controllers and boot them into Maintenance mode:

    `boot_ontap maint`

12. Verify that only storage that will be used by the new DR group is visible to the new controller modules.

    None of the storage that is used by the other DR group should be visible.

13. Return to the beginning of this process to re-cable the second switch fabric.

Configuring ONTAP on the new controllers

You must set up ONTAP on each new controller in the MetroCluster configuration, and then re-create the MetroCluster relationship between the two sites.

Clearing the configuration on a controller module

Before using a new controller module in the MetroCluster configuration, you must clear the existing configuration.

Steps

1. If necessary, halt the node to display the LOADER prompt:

   `halt`

2. At the LOADER prompt, set the environmental variables to default values:

   `set-defaults`

3. Save the environment:

   `saveenv`

4. At the LOADER prompt, launch the boot menu:

   `boot_ontap menu`

5. At the boot menu prompt, clear the configuration:

   `wipeconfig`

   Respond `yes` to the confirmation prompt.

   The node reboots and the boot menu is displayed again.

6. At the boot menu, select option **5** to boot the system into Maintenance mode.

   Respond `yes` to the confirmation prompt.

Assigning disk ownership in AFF systems

If you are using AFF systems in a configuration with mirrored aggregates and the nodes do not have the disks (SSDs) correctly assigned, you should assign half the disks on each shelf to one local node and the other half of the disks to its HA partner node. You should create a configuration in which each node has the same number of disks in its local and remote disk pools.

About this task

The storage controllers must be in Maintenance mode.

This does not apply to configurations which have unmirrored aggregates, an active/passive configuration, or that have an unequal number of disks in local and remote pools.

This task is not required if disks were correctly assigned when received from the factory.

> Pool 0 always contains the disks that are found at the same site as the storage system that owns them, while Pool 1 always contains the disks that are remote to the storage system that owns them.

Steps

1. If you have not done so, boot each system into Maintenance mode.
2. Assign the disks to the nodes located at the first site (site A):

   You should assign an equal number of disks to each pool.

   a. On the first node, systematically assign half the disks on each shelf to pool 0 and the other half to the HA partner's pool 0:
   `disk assign -disk` *`disk-name`* `-p` *`pool`* `-n` *`number-of-disks`*

   If storage controller Controller_A_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1 -n 4
```

b. Repeat the process for the second node at the local site, systematically assigning half the disks on each shelf to pool 1 and the other half to the HA partner's pool 1:
`disk assign -disk disk-name -p pool`

If storage controller Controller_A_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4

*> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1 -n 4
```

3. Assign the disks to the nodes located at the second site (site B):

You should assign an equal number of disks to each pool.

a. On the first node at the remote site, systematically assign half the disks on each shelf to pool 0 and the other half to the HA partner's pool 0:
`disk assign -disk disk-name -p pool`

If storage controller Controller_B_1 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1 -n 4
```

b. Repeat the process for the second node at the remote site, systematically assigning half the disks on each shelf to pool 1 and the other half to the HA partner's pool 1:

`disk assign -disk disk-name -p pool`

If storage controller Controller_B_2 has four shelves, each with 8 SSDs, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0 -n 4
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0 -n 4

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1 -n 4
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1 -n 4
```

4. Confirm the disk assignments:

   `storage show disk`

5. Exit Maintenance mode:

   `halt`

6. Display the boot menu:

   `boot_ontap menu`

7. On each node, select option **4** to initialize all disks.

Assigning disk ownership in non-AFF systems

If the MetroCluster nodes do not have the disks correctly assigned, or if you are using DS460C disk shelves in your configuration, you must assign disks to each of the nodes in the MetroCluster configuration on a shelf-by-shelf basis. You will create a configuration in which each node has the same number of disks in its local and remote disk pools.

About this task

The storage controllers must be in Maintenance mode.

If your configuration does not include DS460C disk shelves, this task is not required if disks were correctly assigned when received from the factory.

> ⓘ Pool 0 always contains the disks that are found at the same site as the storage system that owns them.
>
> Pool 1 always contains the disks that are remote to the storage system that owns them.

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

Assign these disks in the drawer…	To this node and pool…
0 - 2	Local node’s pool 0
3 - 5	HA partner node’s pool 0
6 - 8	DR partner of the local node’s pool 1

9 - 11	DR partner of the HA partner’s pool 1

This disk assignment pattern ensures that an aggregate is minimally affected in case a drawer goes offline.

Steps

1. If you have not done so, boot each system into Maintenance mode.
2. Assign the disk shelves to the nodes located at the first site (site A):

   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. On the first node, systematically assign the local disk shelves to pool 0 and the remote disk shelves to pool 1:

      `disk assign -shelf` *`local-switch-name:shelf-name.port`* `-p` *`pool`*

      If storage controller Controller_A_1 has four shelves, you issue the following commands:

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf1 -p 0
      *> disk assign -shelf FC_switch_A_1:1-4.shelf2 -p 0

      *> disk assign -shelf FC_switch_B_1:1-4.shelf1 -p 1
      *> disk assign -shelf FC_switch_B_1:1-4.shelf2 -p 1
      ```

   b. Repeat the process for the second node at the local site, systematically assigning the local disk shelves to pool 0 and the remote disk shelves to pool 1:

      `disk assign -shelf` *`local-switch-name:shelf-name.port`* `-p` *`pool`*

      If storage controller Controller_A_2 has four shelves, you issue the following commands:

      ```
      *> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
      *> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1

      *> disk assign -shelf FC_switch_A_1:1-4.shelf3 -p 0
      *> disk assign -shelf FC_switch_B_1:1-4.shelf4 -p 1
      ```

3. Assign the disk shelves to the nodes located at the second site (site B):

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

`disk assign -shelf` *`local-switch-nameshelf-name`* `-p` *`pool`*

If storage controller Controller_B_1 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf1 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf2 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf1 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf2 -p 1
```

b. Repeat the process for the second node at the remote site, systematically assigning its local disk shelves to pool 0 and its remote disk shelves to pool 1:

`disk assign -shelf` *`shelf-name`* `-p` *`pool`*

If storage controller Controller_B_2 has four shelves, you issue the following commands:

```
*> disk assign -shelf FC_switch_B_1:1-5.shelf3 -p 0
*> disk assign -shelf FC_switch_B_1:1-5.shelf4 -p 0

*> disk assign -shelf FC_switch_A_1:1-5.shelf3 -p 1
*> disk assign -shelf FC_switch_A_1:1-5.shelf4 -p 1
```

4. Confirm the shelf assignments:

   `storage show shelf`

5. Exit Maintenance mode:

   `halt`

6. Display the boot menu:

   `boot_ontap menu`

7. On each node, select option **4** to initialize all disks.

Verifying the ha-config state of components

In a MetroCluster configuration, the ha-config state of the controller module and chassis components must be set to **mcc** so they boot up properly.

About this task

- The system must be in Maintenance mode.
- This task must be performed on each new controller module.

Steps

1. In Maintenance mode, display the HA state of the controller module and chassis:

```
ha-config show
```

The HA state for all components should be "mcc".

2. If the displayed system state of the controller is not correct, set the HA state for the controller module:

   ```
   ha-config modify controller mcc
   ```

3. If the displayed system state of the chassis is not correct, set the HA state for the chassis:

   ```
   ha-config modify chassis mcc
   ```

4. Repeat these steps on the other replacement node.

Booting the new controllers and joining them to the cluster

To join the new controllers to the cluster, you must boot each new controller module and use the ONTAP cluster setup wizard to identify the cluster will join.

Before you begin

You must have cabled the MetroCluster configuration.

You must not have configured the Service Processor prior to performing this task.

About this task

This task must be performed on each of the new controllers at both clusters in the MetroCluster configuration.

Steps

1. If you have not already done so, power up each node and let them boot completely.

   If the system is in Maintenance mode, issue the `halt` command to exit Maintenance mode, and then issue the following command from the LOADER prompt:

   ```
   boot_ontap
   ```

   The controller module enters the node setup wizard.

   The output should be similar to the following:

```
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.
.
.
.
```

2. Enable the AutoSupport tool by following the directions provided by the system.
3. Respond to the prompts to configure the node management interface.

   The prompts are similar to the following:

```
Enter the node management interface port: [e0M]:
Enter the node management interface IP address: 10.228.160.229
Enter the node management interface netmask: 225.225.252.0
Enter the node management interface default gateway: 10.228.160.1
```

4. Confirm that nodes are configured in high-availability mode:

   `storage failover show -fields mode`

   If not, you must issue the following command on each node, and then reboot the node:

   `storage failover modify -mode ha -node localhost`

   This command configures high availability mode but does not enable storage failover. Storage failover is automatically enabled when you issue the `metrocluster configure` command later in the configuration process.

5. Confirm that you have four ports configured as cluster interconnects:

   `network port show`

   The following example shows output for two controllers in cluster_A. If it is a two-node MetroCluster configuration, the output shows only one node.

```
cluster_A::> network port show
                                                              Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node_A_1
       **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
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
node_A_2
       **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
       e0e       Default      Default          up       1500  auto/1000
       e0f       Default      Default          up       1500  auto/1000
       e0g       Default      Default          up       1500  auto/1000
14 entries were displayed.
```

6. Because you are using the CLI to set up the cluster, exit the Node Setup wizard:

   `exit`

7. Log in to the admin account by using the `admin` user name.
8. Start the Cluster Setup wizard, and then join the existing cluster:

   `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}:`join`
```

9. After you complete the **Cluster Setup** wizard and it exits, verify that the cluster is active and the node is healthy:

   `cluster show`

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

```
cluster_A::> cluster show
Node               Health  Eligibility
------------------ ------- ------------
node_A_1           true    true
node_A_2           true    true
node_A_3           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`.

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.

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.

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.

   The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                             Speed
(Mbps)
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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

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.

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

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

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`*

   The following example assigns ports "e0e" and "e0f" to the failover group "intercluster01" on the system SVM "cluster01":

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Verify that the failover group was created:

   `network interface failover-groups show`

   For complete command syntax, see the man page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

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

ONTAP version	Command
9.6 and later	`network interface create -vserver system_SVM -lif LIF_name -service-policy default-intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover -group failover_group`
9.5 and earlier	`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.

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

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-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 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Verify that the intercluster LIFs are redundant:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster -failover`

In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

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 -service-policy default-intercluster
–failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

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.

   The following example shows the network ports in cluster01:

```
cluster01::> network port show
                                                                      Speed
(Mbps)
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:

In ONTAP 9.6 and later:
`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
In ONTAP 9.5 and earlier:
`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.

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

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

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verify that the intercluster LIFs were created:

In ONTAP 9.6 and later:
`network interface show -service-policy default-intercluster`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster`

For complete command syntax, see the man page.

```
cluster01::> network interface show -service-policy default-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:

In ONTAP 9.6 and later:
`network interface show –service-policy default-intercluster -failover`
In ONTAP 9.5 and earlier:
`network interface show -role intercluster -failover`

For complete command syntax, see the man page.

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

```
cluster01::> network interface show -service-policy default-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
```

Mirroring the root aggregates

You must mirror the root aggregates to provide data protection.

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
```

> 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`*

   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.

Implementing the MetroCluster configuration

You must run the `metrocluster configure -refresh true` command to start data

protection on the nodes that you have added to a MetroCluster configuration.

About this task

You issue the `metrocluster configure -refresh true` command once, on one of the newly added nodes, to refresh the MetroCluster configuration. You do not need to issue the command on each of the sites or nodes.

The `metrocluster configure -refresh true` command automatically pairs the two nodes with the lowest system IDs in each of the two clusters as disaster recovery (DR) partners. In a four-node MetroCluster configuration, there are two DR partner pairs. The second DR pair is created from the two nodes with higher system IDs.

Steps

1. Refresh the MetroCluster configuration:
   a. Enter advanced privilege mode:

      `set -privilege advanced`

   b. Refresh the MetroCluster configuration on one of the new nodes:
      `metrocluster configure -refresh true`

      The following example shows the MetroCluster configuration refreshed on both DR groups:

      ```
      controller_A_2::*> metrocluster configure -refresh true

      [Job 726] Job succeeded: Configure is successful.
      ```

      ```
      controller_A_4::*> metrocluster configure -refresh true

      [Job 740] Job succeeded: Configure is successful.
      ```

   c. Return to admin privilege mode:

      `set -privilege admin`

2. Verify the networking status on site A:

   `network port show`

   The following example shows the network port usage on a four-node MetroCluster configuration:

```
cluster_A::> network port show
                                                          Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Verify the MetroCluster configuration from both sites in the MetroCluster configuration:
   a. Verify the configuration from site A:

      `metrocluster show`

```
cluster_A::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_A         Configuration state configured
                          Mode                normal
Remote: cluster_B         Configuration state configured
                          Mode                normal
```

   b. Verify the configuration from site B:
      `metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                    Entry Name          State
-------------------------- ------------------- -----------
 Local: cluster_B          Configuration state configured
                           Mode                normal
Remote: cluster_A          Configuration state configured
                           Mode                normal
```

Creating a mirrored data aggregate on each node

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

About this task

- You should know what drives 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.
- Drives 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.

  In systems using ADP, aggregates are created using partitions in which each drive is partitioned in to P1, P2 and P3 partitions.
- 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:

   `storage aggregate create -mirror true`

   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 that are to be added to the aggregate
   - Number of drives to include

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 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.

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`*

Configuring FC-to-SAS bridges for health monitoring

About this task

- Third-party SNMP monitoring tools are not supported for FibreBridge bridges.
- Starting with ONTAP 9.8, FC-to-SAS bridges are monitored via in-band connections by default, and additional configuration is not required.

Starting with ONTAP 9.8, the `storage bridge` command is replaced with `system bridge`. The following steps show the `storage bridge` command, but if you are running ONTAP 9.8 or later, the `system bridge` command is preferred.

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:

ONTAP version	Command
9.5 and later	`storage bridge add -address 0.0.0.0 -managed-by in-band -name` *`bridge-name`*

9.4 and earlier	`storage bridge add -address` *`bridge-ip-address`* `-name` *`bridge-name`*

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.

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

```
controller_A_1::> storage bridge show

Bridge              Symbolic Name Is Monitored  Monitor Status
Vendor Model                Bridge WWN
------------------  ------------- ------------  -------------
------ -----------------    ----------
ATTO_10.10.20.10  atto01        true          ok              Atto
FibreBridge 7500N      20000010867038c0
ATTO_10.10.20.11  atto02        true          ok              Atto
FibreBridge 7500N      20000010867033c0
ATTO_10.10.20.12  atto03        true          ok              Atto
FibreBridge 7500N      20000010867030c0
ATTO_10.10.20.13  atto04        true          ok              Atto
FibreBridge 7500N      2000001086703b80

4 entries were displayed

 controller_A_1::>
```

Moving a metadata volume in MetroCluster configurations

You can move a metadata volume from one aggregate to another aggregate in a MetroCluster configuration. You might want to move a metadata volume when the source aggregate is decommissioned or unmirrored, or for other reasons that make the aggregate ineligible.

About this task

- You must have cluster administrator privileges to perform this task.
- The target aggregate must be mirrored and should not be in the degraded state.
- The available space in the target aggregate must be larger than the metadata volume that you are moving.

Steps

1. Set the privilege level to advanced:

   `set -privilege advanced`

2. Identify the metadata volume that should be moved:

   `volume show MDV_CRS*`

```
Cluster_A::*> volume show MDV_CRS*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_A
                       Node_A_1_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_14c00d4ac9f311e7922800a0984395f1_B
                       Node_A_2_aggr1
                                    online     RW         10GB
9.50GB    5%
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_A
                       Node_B_1_aggr1
                                    -          RW            -
-     -
Cluster_A
          MDV_CRS_15035e66c9f311e7902700a098439625_B
                       Node_B_2_aggr1
                                    -          RW            -
-     -
4 entries were displayed.

Cluster_A::>
```

3. Identify an eligible target aggregate:

   `metrocluster check config-replication show-aggregate-eligibility`

   The following command identifies the aggregates in cluster_A that are eligible to host metadata volumes:

```
Cluster_A::*> metrocluster check config-replication show-aggregate-
eligibility

Aggregate Hosted Config Replication Vols Host Addl Vols Comments
------------ ------------------------------------------ --------------
--------
Node_A_1_aggr0 - false Root Aggregate
Node_A_2_aggr0 - false Root Aggregate
Node_A_1_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_A true -
Node_A_2_aggr1 MDV_CRS_1bc7134a5ddf11e3b63f123478563412_B true -
Node_A_1_aggr2 - true
Node_A_2_aggr2 - true
Node_A_1_Aggr3 - false Unable to determine available space of aggregate
Node_A_1_aggr5 - false Unable to determine mirror configuration
Node_A_2_aggr6 - false Mirror configuration does not match requirement
Node_B_1_aggr4 - false NonLocal Aggregate
```

In the previous example, Node_A_1_aggr2 and Node_A_2_aggr2 are eligible.

4. Start the volume move operation:

   `volume move start -vserver *svm_name* -volume *metadata_volume_name* -destination -aggregate *destination_aggregate_name**`

   The following command moves metadata volume "MDV_CRS_14c00d4ac9f311e7922800a0984395f1" from "aggregate Node_A_1_aggr1" to "aggregate Node_A_1_aggr2":

```
Cluster_A::*> volume move start -vserver svm_cluster_A -volume
MDV_CRS_14c00d4ac9f311e7922800a0984395f1
-destination-aggregate aggr_cluster_A_02_01

Warning: You are about to modify the system volume
         "MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A".  This may cause
severe
         performance or stability problems.  Do not proceed unless
directed to
         do so by support.  Do you want to proceed? {y|n}: y
[Job 109] Job is queued: Move
"MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" in Vserver
"svm_cluster_A" to aggregate "aggr_cluster_A_02_01".
Use the "volume move show -vserver svm_cluster_A -volume
MDV_CRS_9da04864ca6011e7b82e0050568be9fe_A" command to view the status
of this operation.
```

5. Verify the state of the volume move operation:

```
volume move show -volume vol_constituent_name
```

6. Return to the admin privilege level:

```
set -privilege admin
```

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
```

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: 9/13/2018 20:41:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
6 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.

   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

Node                  Aggregate                  Check
Result
---------------       --------------------       ---------------------
---------
controller_A_1        controller_A_1_aggr0
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr1
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
                      controller_A_1_aggr2
                                                 mirroring-status
ok
                                                 disk-pool-allocation
ok
                                                 ownership-state
ok
```

```
controller_A_2         controller_A_2_aggr0
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                       controller_A_2_aggr1
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok
                       controller_A_2_aggr2
                                                    mirroring-status
ok
                                                    disk-pool-allocation
ok
                                                    ownership-state
ok

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

Cluster               Check                            Result
--------------------- ------------------------------- ---------
mccint-fas9000-0102
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
mccint-fas9000-0304
                      negotiated-switchover-ready     not-applicable
                      switchback-ready                not-applicable
                      job-schedules                   ok
                      licenses                        ok
                      periodic-check-enabled          ok
10 entries were displayed.
```

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.

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.

Sending a custom AutoSupport message after to adding nodes to the MetroCluster configuration

You should issue an AutoSupport message to notify NetApp technical support that maintenance is complete.

About this task

This task must be performed on each MetroCluster site.

Steps

1. Log in to the cluster at Site_A.
2. Invoke an AutoSupport message indicating the end of the maintenance:

   ```
   system node autosupport invoke -node * -type all -message MAINT=end
   ```

3. Repeat this step on the partner site.

Verifying switchover, healing, and switchback

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

Steps

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

Expanding a four-node MetroCluster IP configuration to an eight-node configuration

Starting with ONTAP 9.9.1, you can add four new nodes to the MetroCluster IP configuration as a second DR group. This creates an eight-node MetroCluster configuration.

Before you begin

- The old and new nodes must be running the same version of ONTAP.
- You must ensure that the old and new platform models are supported for platform mixing.

  NetApp Hardware Universe

- You must ensure that the old and new platform models are both supported by the IP switches.

  NetApp Hardware Universe

- The new nodes must have enough storage to accommodate the data of the old nodes, along with adequate disks for root aggregates and spare disks.

Example naming in this procedure

This procedure uses example names throughout to identify the DR groups, nodes, and switches involved.

DR groups	cluster_A at site_A	cluster_B at site_B
dr_group_1-old	• node_A_1-old • node_A_2-old	• node_B_1-old • node_B_2-old

dr_group_2-new	• node_A_3-new • node_A_4-new	• node_B_3-new • node_B_4-new

Sending a custom AutoSupport message prior to maintenance

Before performing the maintenance, you should issue an AutoSupport message to notify NetApp technical support that maintenance is underway. Informing technical support that maintenance is underway prevents them from opening a case on the assumption that a disruption has occurred.

About this task

This task must be performed on each MetroCluster site.

Steps

1. To prevent automatic support case generation, send an Autosupport message to indicate the upgrade is underway.
   a. Issue the following command:

      ```
      system node autosupport invoke -node * -type all -message "MAINT=10h
      Upgrading old-model to new-model"
      ```

      This example specifies a 10 hour maintenance window. You might want to allow additional time, depending on your plan.

      If the maintenance is completed before the time has elapsed, you can invoke an AutoSupport message indicating the end of the maintenance period:

      ```
      system node autosupport invoke -node * -type all -message MAINT=end
      ```

   b. Repeat the command on the partner cluster.

Verifying the health of the MetroCluster configuration

You must verify the health and connectivity of the MetroCluster configuration prior to performing the transition

Steps

1. Verify the operation of the MetroCluster configuration in ONTAP:
   a. Check whether the system is multipathed:

      ```
      node run -node node-name sysconfig -a
      ```

   b. Check for any health alerts on both clusters:

      ```
      system health alert show
      ```

   c. Confirm the MetroCluster configuration and that the operational mode is normal:

      ```
      metrocluster show
      ```

   d. Perform a MetroCluster check:

```
metrocluster check run
```

e. Display the results of the MetroCluster check:

```
metrocluster check show
```

f. Run Config Advisor.

NetApp Downloads: Config Advisor

g. After running Config Advisor, review the tool's output and follow the recommendations in the output to address any issues discovered.

2. Verify that the cluster is healthy:

```
cluster show -vserver Cluster
```

```
cluster_A::> cluster show -vserver Cluster
Node           Health  Eligibility   Epsilon
-------------- ------  -----------   -------
node_A_1     true    true          false
node_A_2     true    true          false

cluster_A::>
```

3. Verify that all cluster ports are up:

```
network port show -ipspace cluster
```

```
cluster_A::> network port show -ipspace cluster

Node: node_A_1-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

Node: node_A_2-old

                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- --------
e0a       Cluster      Cluster          up   9000  auto/10000 healthy
e0b       Cluster      Cluster          up   9000  auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Verify that all cluster LIFs are up and operational:

   `network interface show -vserver Cluster`

   Each cluster LIF should display true for Is Home and have a Status Admin/Oper of up/up

```
cluster_A::> network interface show -vserver cluster

            Logical      Status     Network           Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node_A_1-old_clus1
                       up/up      169.254.209.69/16  node_A_1   e0a
true
            node_A_1-old_clus2
                       up/up      169.254.49.125/16  node_A_1   e0b
true
            node_A_2-old_clus1
                       up/up      169.254.47.194/16  node_A_2   e0a
true
            node_A_2-old_clus2
                       up/up      169.254.19.183/16  node_A_2   e0b
true

4 entries were displayed.

cluster_A::>
```

5. Verify that auto-revert is enabled on all cluster LIFs:

   `network interface show -vserver Cluster -fields auto-revert`

```
cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
           node_A_1-old_clus1
                        true
           node_A_1-old_clus2
                        true
           node_A_2-old_clus1
                        true
           node_A_2-old_clus2
                        true

    4 entries were displayed.

cluster_A::>
```

Removing the configuration from monitoring applications

If the existing configuration is monitored with the MetroCluster Tiebreaker software, the ONTAP Mediator or other third-party applications (for example, ClusterLion) that can initiate a switchover, you must remove the MetroCluster configuration from the monitoring software prior to upgrade.

Steps

1. Remove the existing MetroCluster configuration from Tiebreaker, Mediator, or other software that can initiate switchover.

If you are using…	Use this procedure…
Tiebreaker	Removing MetroCluster Configurations in the *MetroCluster Tiebreaker Installation and Configuration Guide*
Mediator	Issue the following command from the ONTAP prompt: `metrocluster configuration-settings mediator remove`
Third-party applications	Refer to the product documentation.

2. Remove the existing MetroCluster configuration from any third-party application that can initiate switchover.

   Refer to the documentation for the application.

Preparing the new controller modules

You must prepare the four new MetroCluster nodes and install the correct ONTAP version.

About this task

This task must be performed on each of the new nodes:

- node_A_3-new
- node_A_4-new
- node_B_3-new
- node_B_4-new

In these steps, you clear the configuration on the nodes and clear the mailbox region on new drives.

Steps

1. Rack the new controllers.
2. Cable the new MetroCluster IP nodes to the IP switches as shown in the *MetroCluster Installation and Configuration Guide.*

   Cabling the IP switches

3. Configure the MetroCluster IP nodes using the following sections of the *MetroCluster Installation and Configuration Guide.*
   a. Gathering required information
   b. Restoring system defaults on a controller module
   c. Verifying the ha-config state of components
   d. Manually assigning drives for pool 0 (ONTAP 9.4 and later)
4. From Maintenance mode, issue the halt command to exit Maintenance mode, and then issue the boot_ontap command to boot the system and get to cluster setup.

   Do not complete the cluster wizard or node wizard at this time.

Joining the new nodes to the clusters

You must add the four new MetroCluster IP nodes to the existing MetroCluster configuration.

About this task

You must perform this task on both clusters.

Steps

1. Add the new MetroCluster IP nodes to the existing MetroCluster configuration.
   a. Join the first new MetroCluster IP node (node_A_1-new) to the existing MetroCluster IP configuration.

```
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.

This system will send event messages and periodic 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}: yes

Enter the node management interface port [e0M]: 172.17.8.93

172.17.8.93 is not a valid port.

The physical port that is connected to the node management network.
Examples of
node management ports are "e4a" or "e0M".

You can type "back", "exit", or "help" at any question.


Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.93
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.93
has been created.

Use your web browser to complete cluster setup by accessing
https://172.17.8.93

Otherwise, press Enter to complete cluster setup using the command
line
interface:
```

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


Existing cluster interface configuration found:

Port     MTU      IP               Netmask
e0c      9000     169.254.148.217 255.255.0.0
e0d      9000     169.254.144.238 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: yes
.
.
.
```

b. Join the second new MetroCluster IP node (node_A_2-new) to the existing MetroCluster IP configuration.

2. Repeat these steps to join node_B_1-new and node_B_2-new to cluster_B.

Configuring intercluster LIFs, creating the MetroCluster interfaces, and mirroring root aggregates

You must create cluster peering LIFs, create the MetroCluster interfaces on the new MetroCluster IP nodes.

About this task

The home port used in the examples are platform-specific. You should use the appropriate home port specific to MetroCluster IP node platform.

Steps

1. On the new MetroCluster IP nodes, configure the intercluster LIFs using the procedures in the *MetroCluster IP Installation and Configuration Guide*.

   Configuring intercluster LIFs on dedicated ports

   Configuring intercluster LIFs on shared data ports

2. On each site, verify that cluster peering is configured:

   `cluster peer show`

   The following example shows the cluster peering configuration on cluster_A:

```
cluster_A:> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_B                  1-80-000011           Available      ok
```

The following example shows the cluster peering configuration on cluster_B:

```
cluster_B:> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
cluster_A                  1-80-000011           Available      ok
cluster_B::>
```

3. Create the DR group for the MetroCluster IP nodes:

   `metrocluster configuration-settings dr-group create -partner-cluster`

   For more information on the MetroCluster configuration settings and connections, see the *MetroCluster IP Installation and Configuration Guide*.

   Considerations for MetroCluster IP configurations

   Creating the DR group

```
cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster
cluster_B -local-node node_A_1-new -remote-node node_B_1-new
[Job 259] Job succeeded: DR Group Create is successful.
cluster_A::>
```

4. Verify that the DR group was created.

   `metrocluster configuration-settings dr-group show`

```
cluster_A::> metrocluster configuration-settings dr-group show

DR Group ID Cluster                    Node               DR Partner
Node
----------- -------------------------- ------------------
------------------
1           cluster_A
                                       node_A_1-old        node_B_1-old
                                       node_A_2-old        node_B_2-old
            cluster_B
                                       node_B_1-old        node_A_1-old
                                       node_B_2-old        node_A_2-old
2           cluster_A
                                       node_A_1-new        node_B_1-new
                                       node_A_2-new        node_B_2-new
            cluster_B
                                       node_B_1-new        node_A_1-new
                                       node_B_2-new        node_A_2-new
8 entries were displayed.

cluster_A::>
```

5. Configure the MetroCluster IP interfaces for the newly joined MetroCluster IP nodes:

```
metrocluster configuration-settings interface create -cluster-name
```

> ◦ Starting with ONTAP 9.8, certain platforms use a VLAN for the MetroCluster IP interface. By default, each of the two ports use a different VLAN: 10 and 20. You can also specify a different (non-default) VLAN higher than 100 (between 101 and 4095) using the `-vlan-id parameter` in the `metrocluster configuration-settings interface create` command.
>
> ◦ Starting with ONTAP 9.9.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter when creating MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.

The following platform models use VLANs and allow configuration of a non-default VLAN ID.

AFF platforms	FAS platforms
• AFF A220 • AFF A250 • AFF A400	• FAS2750 • FAS500f • FAS8300 • FAS8700

You can configure the MetroCluster IP interfaces from either cluster. Also, starting with ONTAP 9.1.1, if you are using a layer 3 configuration, you must also specify the `-gateway` parameter to create MetroCluster IP interfaces. Refer to Considerations for layer 3 wide-area networks.

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1a -address
172.17.26.10 -netmask 255.255.255.0
[Job 260] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1-new -home-port e1b -address
172.17.27.10 -netmask 255.255.255.0
[Job 261] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1a -address
172.17.26.11 -netmask 255.255.255.0
[Job 262] Job succeeded: Interface Create is successful.

cluster_A::> :metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2-new -home-port e1b -address
172.17.27.11 -netmask 255.255.255.0
[Job 263] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1a -address
172.17.26.12 -netmask 255.255.255.0
[Job 264] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1-new -home-port e1b -address
172.17.27.12 -netmask 255.255.255.0
[Job 265] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1a -address
172.17.26.13 -netmask 255.255.255.0
[Job 266] Job succeeded: Interface Create is successful.

cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2-new -home-port e1b -address
172.17.27.13 -netmask 255.255.255.0
[Job 267] Job succeeded: Interface Create is successful.
```

6. Verify the MetroCluster IP interfaces are created:

   `metrocluster configuration-settings interface show`

```
cluster_A::>metrocluster configuration-settings interface show

DR
Config
Group Cluster Node    Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1     cluster_A
             node_A_1-old
                 Home Port: e1a
                      172.17.26.10    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.10    255.255.255.0   -
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.26.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.11    255.255.255.0   -
completed
      cluster_B
             node_B_1-old
                 Home Port: e1a
                      172.17.26.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.13    255.255.255.0   -
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.26.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.27.12    255.255.255.0   -
completed
2     cluster_A
             node_A_3-new
                 Home Port: e1a
                      172.17.28.10    255.255.255.0   -
```

```
completed
                 Home Port: e1b
                      172.17.29.10    255.255.255.0   -
completed
              node_A_3-new
                 Home Port: e1a
                      172.17.28.11    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.11    255.255.255.0   -
completed
      cluster_B
             node_B_3-new
                 Home Port: e1a
                      172.17.28.13    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.13    255.255.255.0   -
completed
              node_B_3-new
                 Home Port: e1a
                      172.17.28.12    255.255.255.0   -
completed
                 Home Port: e1b
                      172.17.29.12    255.255.255.0   -
completed
8 entries were displayed.

cluster_A>
```

7. Connect the MetroCluster IP interfaces:

   `metrocluster configuration-settings connection connect`

   > This command might take several minutes to complete.

```
cluster_A::> metrocluster configuration-settings connection connect

cluster_A::>
```

8. Verify the connections are properly established: `metrocluster configuration-settings connection show`

```
cluster_A::> metrocluster configuration-settings connection show
```

```
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_A
              node_A_1-old
                 Home Port: e1a
                      172.17.28.10    172.17.28.11    HA Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.12    DR Partner
completed
                 Home Port: e1a
                      172.17.28.10    172.17.28.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.11    HA Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.12    DR Partner
completed
                 Home Port: e1b
                      172.17.29.10    172.17.29.13    DR Auxiliary
completed
              node_A_2-old
                 Home Port: e1a
                      172.17.28.11    172.17.28.10    HA Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.13    DR Partner
completed
                 Home Port: e1a
                      172.17.28.11    172.17.28.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.10    HA Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.13    DR Partner
completed
                 Home Port: e1b
                      172.17.29.11    172.17.29.12    DR Auxiliary
completed

DR                    Source          Destination
```

```
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_2-old
                 Home Port: e1a
                      172.17.28.13    172.17.28.12    HA Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.11    DR Partner
completed
                 Home Port: e1a
                      172.17.28.13    172.17.28.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.12    HA Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.11    DR Partner
completed
                 Home Port: e1b
                      172.17.29.13    172.17.29.10    DR Auxiliary
completed
              node_B_1-old
                 Home Port: e1a
                      172.17.28.12    172.17.28.13    HA Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.10    DR Partner
completed
                 Home Port: e1a
                      172.17.28.12    172.17.28.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.13    HA Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.10    DR Partner
completed
                 Home Port: e1b
                      172.17.29.12    172.17.29.11    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
```

```
Config State
----- ------- ------- -------------- -------------- ------------
------------
2     cluster_A
              node_A_1-new**
                 Home Port: e1a
                      172.17.26.10    172.17.26.11    HA Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.12    DR Partner
completed
                 Home Port: e1a
                      172.17.26.10    172.17.26.13    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.11    HA Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.12    DR Partner
completed
                 Home Port: e1b
                      172.17.27.10    172.17.27.13    DR Auxiliary
completed
              node_A_2-new
                 Home Port: e1a
                      172.17.26.11    172.17.26.10    HA Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.13    DR Partner
completed
                 Home Port: e1a
                      172.17.26.11    172.17.26.12    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.10    HA Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.13    DR Partner
completed
                 Home Port: e1b
                      172.17.27.11    172.17.27.12    DR Auxiliary
completed

DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
```

```
----- ------- ------- --------------- --------------- ------------
------------
2     cluster_B
              node_B_2-new
                 Home Port: e1a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e1a
                      172.17.26.13    172.17.26.11    DR Partner
completed
                 Home Port: e1a
                      172.17.26.13    172.17.26.10    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.12    HA Partner
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.11    DR Partner
completed
                 Home Port: e1b
                      172.17.27.13    172.17.27.10    DR Auxiliary
completed
              node_B_1-new
                 Home Port: e1a
                      172.17.26.12    172.17.26.13    HA Partner
completed
                 Home Port: e1a
                      172.17.26.12    172.17.26.10    DR Partner
completed
                 Home Port: e1a
                      172.17.26.12    172.17.26.11    DR Auxiliary
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.13    HA Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.10    DR Partner
completed
                 Home Port: e1b
                      172.17.27.12    172.17.27.11    DR Auxiliary
completed
48 entries were displayed.

cluster_A::>
```

9. Verify disk auto-assignment and partitioning:

```
disk show -pool Pool1
```

```
cluster_A::> disk show -pool Pool1
                          Usable           Disk    Container   Container
Disk                        Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
1.10.4                        -    10   4 SAS     remote      -
node_B_2
1.10.13                       -    10  13 SAS     remote      -
node_B_2
1.10.14                       -    10  14 SAS     remote      -
node_B_1
1.10.15                       -    10  15 SAS     remote      -
node_B_1
1.10.16                       -    10  16 SAS     remote      -
node_B_1
1.10.18                       -    10  18 SAS     remote      -
node_B_2
...
2.20.0                  546.9GB    20   0 SAS     aggregate   aggr0_rha1_a1
node_a_1
2.20.3                  546.9GB    20   3 SAS     aggregate   aggr0_rha1_a2
node_a_2
2.20.5                  546.9GB    20   5 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.6                  546.9GB    20   6 SAS     aggregate   rha1_a1_aggr1
node_a_1
2.20.7                  546.9GB    20   7 SAS     aggregate   rha1_a2_aggr1
node_a_2
2.20.10                 546.9GB    20  10 SAS     aggregate   rha1_a1_aggr1
node_a_1
...
43 entries were displayed.

cluster_A::>
```

10. Mirror the root aggregates:

```
storage aggregate mirror -aggregate aggr0_node_A_1-new
```

ⓘ You must complete this step on each MetroCluster IP node.

```
cluster_A::> aggr mirror -aggregate aggr0_node_A_1-new

Info: Disks would be added to aggregate "aggr0_node_A_1-new"on node
"node_A_1-new"
      in the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.0                    SAS               -
-
          parity     4.20.3                    SAS               -
-
          data       4.20.1                    SAS         546.9GB
558.9GB

      Aggregate capacity available forvolume use would be 467.6GB.

Do you want to continue? {y|n}: y

cluster_A::>
```

11. Verify that the root aggregates are mirrored:

`storage aggregate show`

```
cluster_A::> aggr show

Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_node_A_1-old
           349.0GB   16.84GB   95% online       1 node_A_1-old
raid_dp,

mirrored,

normal
```

```
aggr0_node_A_2-old
           349.0GB   16.84GB   95% online       1 node_A_2-old
raid_dp,

mirrored,

normal
aggr0_node_A_1-new
           467.6GB   22.63GB   95% online       1 node_A_1-new
raid_dp,

mirrored,

normal
aggr0_node_A_2-new
           467.6GB   22.62GB   95% online       1 node_A_2-new
raid_dp,

mirrored,

normal
aggr_data_a1
            1.02TB    1.01TB    1% online       1 node_A_1-old
raid_dp,

mirrored,

normal
aggr_data_a2
            1.02TB    1.01TB    1% online       1 node_A_2-old
raid_dp,

mirrored,
```

Finalizing the addition of the new nodes

You must incorporate the new DR group into the MetroCluster configuration and create mirrored data aggregates on the new nodes.

Steps

1. Create mirrored data aggregates on each of the new MetroCluster nodes:

   `storage aggregate create -aggregate *aggregate-name* -node *node-name* -diskcount *no-of-disks* -mirror true`

> You must create at least one mirrored data aggregate per site. It is recommended to have two mirrored data aggregates per site on MetroCluster IP nodes to host the MDV volumes, however a single aggregate per site is supported (but not recommended). It is support that one site of the MetroCluster has a single mirrored data aggregate and the other site has more than one mirrored data aggregate.

The following example shows the creation of an aggregate on node_A_1-new.

```
cluster_A::> storage aggregate create -aggregate data_a3 -node node_A_1-
new -diskcount 10 -mirror t

Info: The layout for aggregate "data_a3" on node "node_A_1-new" would
be:

      First Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    5.10.15                   SAS               -
-
          parity     5.10.16                   SAS               -
-
          data       5.10.17                   SAS         546.9GB
547.1GB
          data       5.10.18                   SAS         546.9GB
558.9GB
          data       5.10.19                   SAS         546.9GB
558.9GB

      Second Plex

        RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                            Usable
Physical
          Position   Disk                      Type           Size
Size
          ---------- ------------------------- ---------- --------
--------
          dparity    4.20.17                   SAS               -
-
          parity     4.20.14                   SAS               -
```

```
-
          data       4.20.18                   SAS        546.9GB
547.1GB
          data       4.20.19                   SAS        546.9GB
547.1GB
          data       4.20.16                   SAS        546.9GB
547.1GB

      Aggregate capacity available for volume use would be 1.37TB.

Do you want to continue? {y|n}: y
[Job 440] Job succeeded: DONE

cluster_A::>
```

2. Refresh the MetroCluster configuration:
   a. Enter advanced privilege mode:

      `set -privilege advanced`

   b. Refresh the MetroCluster configuration on one of the new nodes:

      `metrocluster configure`

      The following example shows the MetroCluster configuration refreshed on both DR groups:

      ```
      cluster_A::*> metrocluster configure -refresh true

      [Job 726] Job succeeded: Configure is successful.
      ```

   c. Return to admin privilege mode:

      `set -privilege admin`

3. Verify that the nodes are added to their DR group.

```
cluster_A::*> metrocluster node show

DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1-old        configured     enabled   normal
              node_A_2-old        configured     enabled   normal
      cluster_B
              node_B_1-old        configured     enabled   normal
              node_B_2-old        configured     enabled   normal
2     cluster_A
              node_A_3-new        configured     enabled   normal
              node_A_4-new        configured     enabled   normal
      cluster_B
              node_B_3-new        configured     enabled   normal
              node_B_4-new        configured     enabled   normal
8 entries were displayed.

cluster_A::*>
```

4. Move the MDV_CRS volumes from the old nodes to the new nodes in advanced privilege.
   a. Display the volumes to identify the MDV volumes:

      > ⓘ If you have a single mirrored data aggregate per site then move both the MDV volumes to this single aggregate. If you have two or more mirrored data aggregates, then move each MDV volume to a different aggregate.

      The following example shows the MDV volumes in the `volume show` output:

```
cluster_A::> volume show
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
...

cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_A
                       aggr_b1      -          RW            -
-     -
cluster_A   MDV_CRS_2c78e009ff5611e9b0f300a0985ef8c4_B
                       aggr_b2      -          RW            -
-     -
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_A
                       aggr_a1      online     RW         10GB
9.50GB    0%
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
...
11 entries were displayed.mple
```

b. Set the advanced privilege level:

```
set -privilege advanced
```

c. Move the MDV volumes, one at a time:

```
volume move start -volume mdv-volume -destination-aggregate aggr-on-new-node
-vserver vserver-name
```

The following example shows the command and output for moving "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" to aggregate "data_a3" on "node_A_3".

```
cluster_A::> vol move start -volume
MDV_CRS_d6b0b313ff5611e9837100a098544e51_A -destination-aggregate
data_a3 -vserver cluster_A

Warning: You are about to modify the system volume
         "MDV_CRS_d6b0b313ff5611e9837100a098544e51_A". This might
cause severe
         performance or stability problems. Do not proceed unless
directed to
         do so by support. Do you want to proceed? {y|n}: y
[Job 494] Job is queued: Move
"MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" in Vserver "cluster_A"
to aggregate "data_a3". Use the "volume move show -vserver cluster_A
-volume MDV_CRS_d6b0b313ff5611e9837100a098544e51_A" command to view
the status of this operation.
```

d. Use the volume show command to check that the MDV volume has been successfully moved:

`volume show` *`mdv-name`*

The following output shows that the MDV volume has been successfully moved.

```
cluster_A::> vol show MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
Vserver     Volume       Aggregate    State      Type       Size
Available Used%
---------   ------------ ------------ ---------- ---- ----------
---------- -----
cluster_A   MDV_CRS_d6b0b313ff5611e9837100a098544e51_B
                       aggr_a2      online     RW         10GB
9.50GB    0%
```

e. Return to admin mode:

`set -privilege admin`

5. Move epsilon from an old node to a new node:

a. Identify which node currently has epsilon:

`cluster show -fields epsilon`

```
cluster_B::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-old      true
node_A_2-old      false
node_A_3-new      false
node_A_4-new      false
4 entries were displayed.
```

b. Set epsilon to false on the old node (node_A_1-old):

`cluster modify -node *old-node* -epsilon false*`

c. Set epsilon to true on the new node (node_A_3-new):

`cluster modify -node *new-node* -epsilon true`

d. Verify that epsilon has moved to the correct node:

`cluster show -fields epsilon`

```
cluster_A::> cluster show -fields epsilon
node             epsilon
---------------- -------
node_A_1-old      false
node_A_2-old      false
node_A_3-new      true
node_A_4-new      false
4 entries were displayed.
```

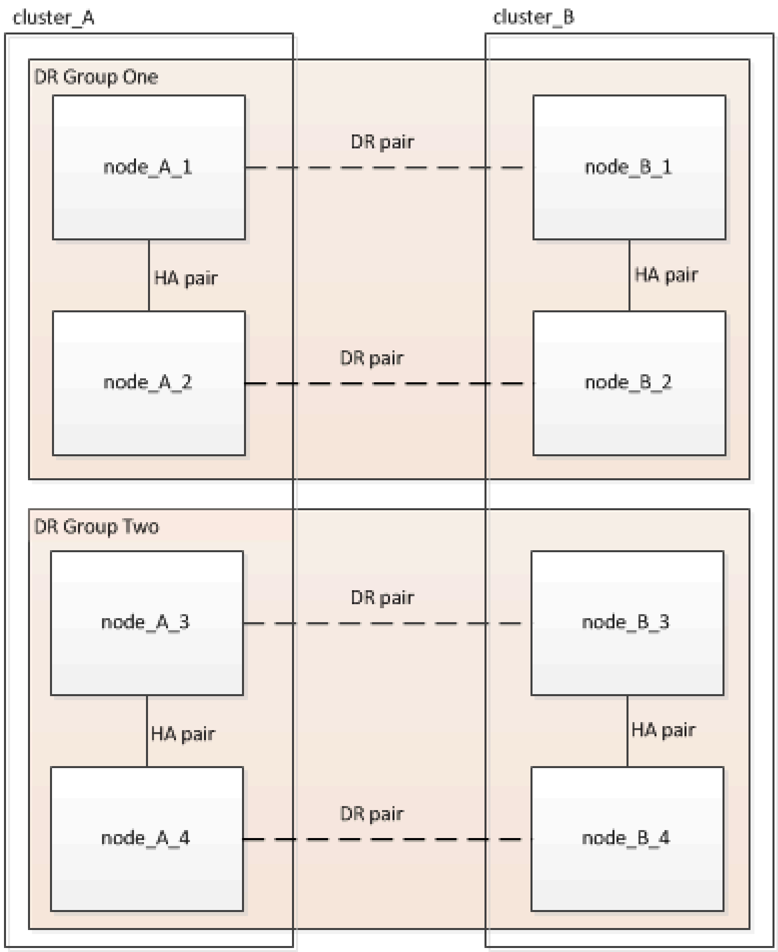
Removing a Disaster Recovery group

Starting with ONTAP 9.8, you can remove a DR group from an eight-node MetroCluster configuration to create a four-node MetroCluster configuration.

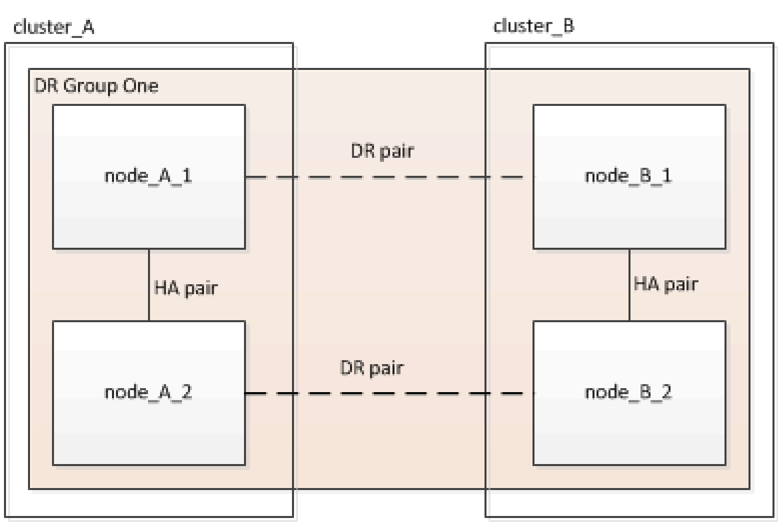
This procedure is supported on ONTAP 9.8 and later. On earlier versions of ONTAP, please contact technical support to remove a DR group.

NetApp Support

An eight-node configuration includes eight-nodes organized as two four-node DR groups.



By removing a DR Group, four nodes remain in the configuration.



Removing the DR group nodes from each cluster

- You must perform this step on both clusters.
- The `metrocluster remove-dr-group` command is supported only on ONTAP 9.8 and later.

1. Prepare for the removal of the DR group, if you haven't already.
   a. Move all data volumes to another DR group.

b. Move all MDV_CRS metadata volumes to another DR group. Follow the steps in the following procedure: Moving a metadata volume in MetroCluster configurations

c. Delete all MDV_aud metadata volumes that might exist in the DR group to be removed.

d. Delete all data aggregates in the DR group to be removed as shown in the following example:

```
ClusterA::> storage aggregate show -node ClusterA-01, ClusterA-02
-fields aggregate ,node
ClusterA::> aggr delete -aggregate aggregate_name
ClusterB::> storage aggregate show -node ClusterB-01, ClusterB-02
-fields aggregate ,node
ClusterB::> aggr delete -aggregate aggregate_name
```

> Root aggregates are not deleted.

e. Migrate all data LIFs to home nodes in another DR group.
`network interface show -home-node` *`old_node`*

`network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

f. Migrate the cluster management LIF to a home node in another DR group.

`network interface show -role cluster-mgmt`

`network interface modify -vserver` *`svm-name`* `-lif` *`data-lif`* `-home-port` *`port-id`*

Node management and inter-cluster LIFs are not migrated.

g. Transfer epsilon to a node in another DR group if required.

```
ClusterA::> set advanced
ClusterA::*> cluster show
Move epsilon if needed
ClusterA::*> cluster modify -node nodename -epsilon false
ClusterA::*> cluster modify -node nodename -epsilon true

ClusterB::> set advanced
ClusterB::*> cluster show
ClusterB::*> cluster modify -node nodename -epsilon false
ClusterB::*> cluster modify -node nodename -epsilon true
ClusterB::*> set admin
```

2. Identify and remove the DR group.

a. Identify the correct DR group for removal:

```
metrocluster node show
```

b. Remove the DR group nodes:

```
metrocluster remove-dr-group -dr-group-id 1
```

The following example shows the removal of the DR group configuration on cluster_A.

```
cluster_A::*>

Warning: Nodes in the DR group that are removed from the
MetroCluster
         configuration will lose their disaster recovery
protection.

         Local nodes "node_A_1-FC, node_A_2-FC"will be removed
from the
         MetroCluster configuration. You must repeat the operation
on the
         partner cluster "cluster_B"to remove the remote nodes in
the DR group.
Do you want to continue? {y|n}: y

Info: The following preparation steps must be completed on the
local and partner
      clusters before removing a DR group.

      1. Move all data volumes to another DR group.
      2. Move all MDV_CRS metadata volumes to another DR group.
      3. Delete all MDV_aud metadata volumes that may exist in the
DR group to
      be removed.
      4. Delete all data aggregates in the DR group to be removed.
Root
      aggregates are not deleted.
      5. Migrate all data LIFs to home nodes in another DR group.
      6. Migrate the cluster management LIF to a home node in
another DR group.
      Node management and inter-cluster LIFs are not migrated.
      7. Transfer epsilon to a node in another DR group.

      The command is vetoed if the preparation steps are not
completed on the
      local and partner clusters.
Do you want to continue? {y|n}: y
[Job 513] Job succeeded: Remove DR Group is successful.

cluster_A::*>
```

3. Repeat the previous step on the partner cluster.
4. If in a MetroCluster IP configuration, remove the MetroCluster connections on the nodes of the old DR group.

These commands can be issued from either cluster and apply to the entire DR group spanning both the clusters.

a. Disconnect the connections:

```
metrocluster configuration-settings connection disconnect dr-group-id
```

b. Delete the MetroCluster interfaces on the nodes of the old DR group:

```
metrocluster configuration-settings interface delete
```

c. Delete the old DR group's configuration.
```
metrocluster configuration-settings dr-group delete
```

5. Unjoin the nodes in the old DR group.

   You must perform this step on each cluster.

   a. Set the advanced privilege level:

   ```
   set -privilege advanced
   ```

   b. Unjoin the node:
   ```
   cluster unjoin -node node-name
   ```

      Repeat this step for the other local node in the old DR group.

   c. Set the admin privilege level:
   ```
   set -privilege admin
   ```

6. Re-enable cluster HA in the new DR group:

   ```
   cluster ha modify -configured true
   ```

   You must perform this step on each cluster.

7. Halt, power down, and remove the old controller modules and storage shelves.

Where to find additional information

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

MetroCluster and miscellaneous guides

Guide	Content
ONTAP 9 Documentation Center	• All MetroCluster guides

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
Stretch MetroCluster installation and configuration	• Stretch MetroCluster architecture • Cabling the configuration • Configuring the FC-to-SAS bridges • Configuring the MetroCluster in ONTAP
MetroCluster management and disaster recovery	• Understanding the MetroCluster configuration • Switchover, healing and switchback • Disaster recovery
Maintain MetroCluster Components	• Guidelines for maintenance in a MetroCluster FC configuration • Hardware replacement or upgrade and firmware upgrade procedures for FC-to-SAS bridges and FC switches • Hot-adding a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Hot-removing a disk shelf in a fabric-attached or stretch MetroCluster FC configuration • Replacing hardware at a disaster site in a fabric-attached or stretch MetroCluster FC configuration • Expanding a two-node fabric-attached or stretch MetroCluster FC configuration to a four-node MetroCluster configuration. • Expanding a four-node fabric-attached or stretch MetroCluster FC configuration to an eight-node MetroCluster FC configuration.
MetroCluster Upgrade, Transition, and Expansion Guide	• Upgrading or refreshing a MetroCluster configuration • Transitioning from a MetroCluster FC configuration to a MetroCluster IP configuration • Expanding a MetroCluster configuration by adding additional nodes
MetroCluster Tiebreaker Software Installation and Configuration Guide	• Monitoring the MetroCluster configuration with the MetroCluster Tiebreaker software

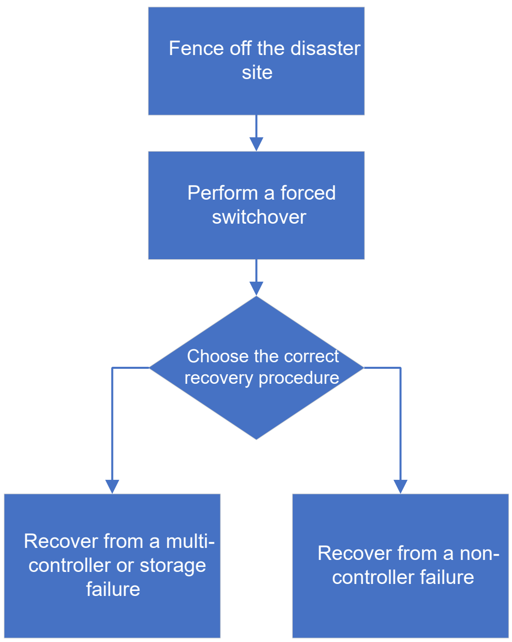
AFF and FAS Documentation Center ⓘ The standard storage shelf maintenance procedures can be used with MetroCluster IP configurations.	• Hot-adding a disk shelf • Hot-removing a disk shelf
Copy-based transition	• Transitioning data from 7-Mode storage systems to clustered storage systems
ONTAP concepts	• How mirrored aggregates work

MetroCluster® Management and Disaster Recovery Guide

This content describes how to perform MetroCluster switchover and switchback operations, both in planned maintenance operations or in the event of a disaster.

Workflow for disaster recovery

Use the workflow to perform disaster recovery.



Performing a forced switchover after a disaster

If a disaster has occurred, there are steps you must perform on both the disaster cluster and the surviving cluster after the switchover to ensure safe and continued data service.

Determining if a disaster has occurred is done by:

- An administrator
- The MetroCluster Tiebreaker software, if it is configured
- The ONTAP Mediator software, if it is configured

Fencing off the disaster site

After the disaster, if the disaster site nodes must be replaced, you must halt them to prevent the site from resuming service. Otherwise, you risk the possibility of data corruption if clients start accessing the nodes before the replacement procedure is completed.

Step

1. Halt the nodes at the disaster site and keep them powered down or at the LOADER prompt until directed to boot ONTAP:

   ```
   system node halt -node disaster-site-node-name
   ```

   If the disaster site nodes have been destroyed or cannot be halted, turn off power to the nodes and do not boot the replacement nodes until directed to in the recovery procedure.

Performing a forced switchover

The switchover process, in addition to providing nondisruptive operations during testing and maintenance, enables you to recover from a site failure with a single command.

Before you begin

- At least one of the surviving site nodes must up and running before you perform the switchover.
- All previous configuration changes must be complete before performing a switchback operation.

  This is to avoid competition with the negotiated switchover or switchback operation.

> SnapMirror and SnapVault configurations are deleted automatically.

About this task

The `metrocluster switchover` command switches over the nodes in all DR groups in the MetroCluster configuration. For example, in an eight-node MetroCluster configuration, it switches over the nodes in both DR groups.

Steps

1. Implement the switchover:

   ```
   metrocluster switchover -forced-on-disaster true
   ```

   The operation can take a period of minutes to complete.

2. Answer `y` when prompted to continue with the switchover.
3. Verify that the switchover was completed successfully by running the metrocluster operation show command.

```
mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: in-progress
   End time: -
     Errors:

mcc1A::> metrocluster operation show
  Operation: switchover
 Start time: 10/4/2012 19:04:13
      State: successful
   End time: 10/4/2012 19:04:22
     Errors: -
```

If the switchover is vetoed, you have the option of reissuing the `metrocluster switchover-forced-on-disaster true` command with the `--override-vetoes` option. If you use this optional parameter, the system overrides any soft vetoes that prevented the switchover.

After you finish

SnapMirror relationships need to be reestablished after switchover.

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.

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 the `-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.

Related information

Monitoring and protecting database validity by using NVFAIL

Choosing the correct recovery procedure

After a failure in a MetroCluster configuration, you must select the correct recovery procedure. Use the following table and examples to select the appropriate recovery procedure.

Scope of failures at disaster site	Procedure
• No controller module failure • Other hardware has failed	Recovering from a non-controller failure
• Single controller module failure or failure of FRU components within the controller module • Drives have not failed	If a failure is limited to a single controller module, you must use the controller module FRU replacement procedure for the platform model. In a four or eight-node MetroCluster configuration, such a failure is isolated to the local HA pair. **Note:** The controller module FRU replacement procedure can be used in a two-node MetroCluster configuration if there are no drive or other hardware failures. AFF and FAS Documentation Center
• Single controller module failure or failure of FRU components within the controller module • Drives have failed	Recovering from a multi-controller or storage failure
• Single controller module failure or failure of FRU components within the controller module • Drives have not failed • Additional hardware outside the controller module has failed	Recovering from a multi-controller or storage failure You should skip all steps for drive assignment.
• Multiple controller module failure (with or without additional failures) within a DR group	Recovering from a multi-controller or storage failure

Controller module failure scenarios during MetroCluster FC-to-IP Transition

The recovery procedure can be used if a site failure occurs during transition. However, it can only be used if the configuration is a stable mixed configuration, with the FC DR group and IP DR group both fully configured. The output of the `metrocluster node show` command should show both DR groups with all eight nodes.

If the failure occurred during transition when the nodes are in the process of being added or removed, you must contact technical support.

Controller module failure scenarios in eight-node MetroCluster configurations

Failure scenarios:

- Single controller module failures in a single DR group
- Two controller module failures in a single DR group
- Single controller module failures in separate DR groups
- Three controller module failures spread across the DR groups

Single controller module failures in a single DR group

In this case the failure is limited to an HA pair.

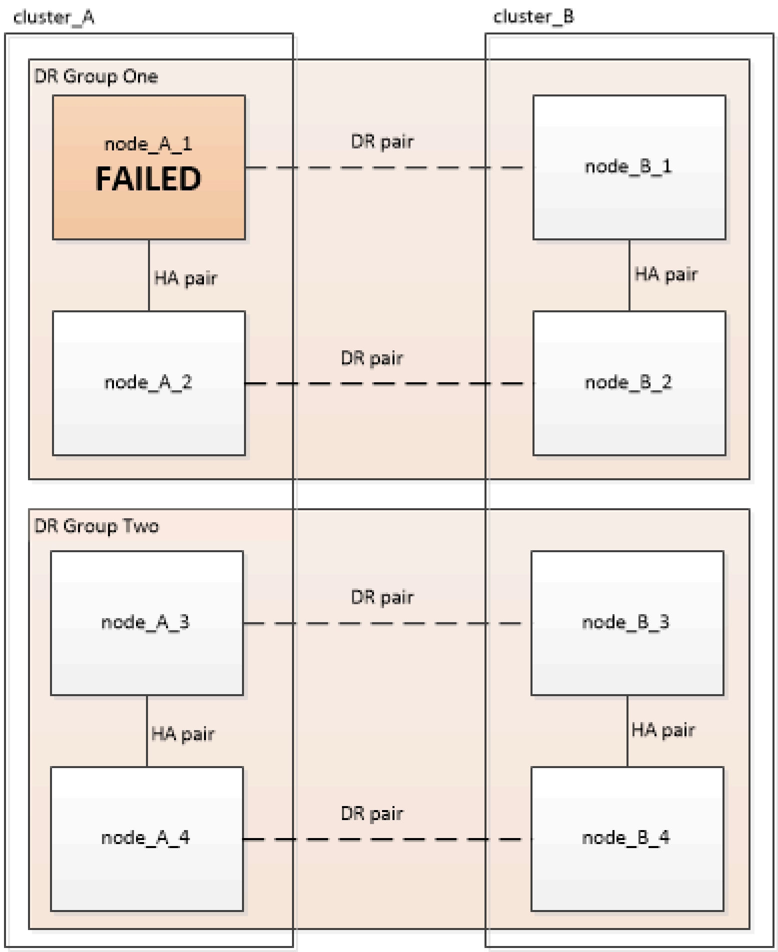
- If no storage requires replacement, you can use the controller module FRU replacement procedure for the platform model.

  AFF and FAS Documentation Center

- If storage requires replacement, you can use the multi-controller module recovery procedure.

  Recovering from a multi-controller or storage failure

  This scenario applies to four-node MetroCluster configurations also.

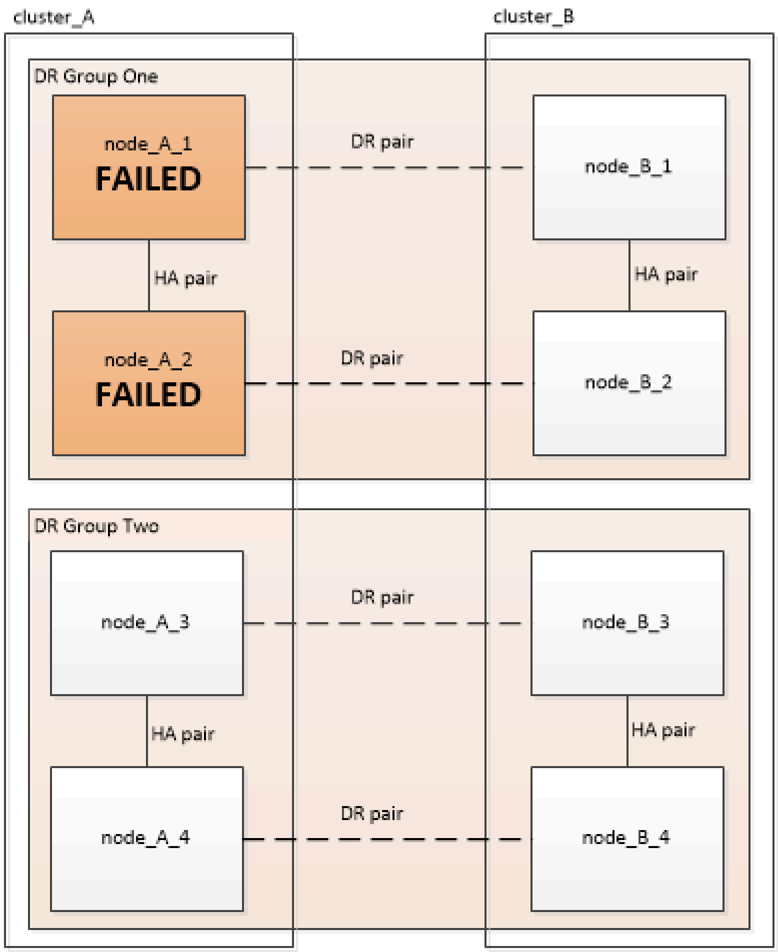


Two controller module failures in a single DR group

In this case the failure requires a switchover. You can use the multi-controller module failure recovery procedure.

Recovering from a multi-controller or storage failure

This scenario applies to four-node MetroCluster configurations also.



Single controller module failures in separate DR groups

In this case the failure is limited to separate HA pairs.

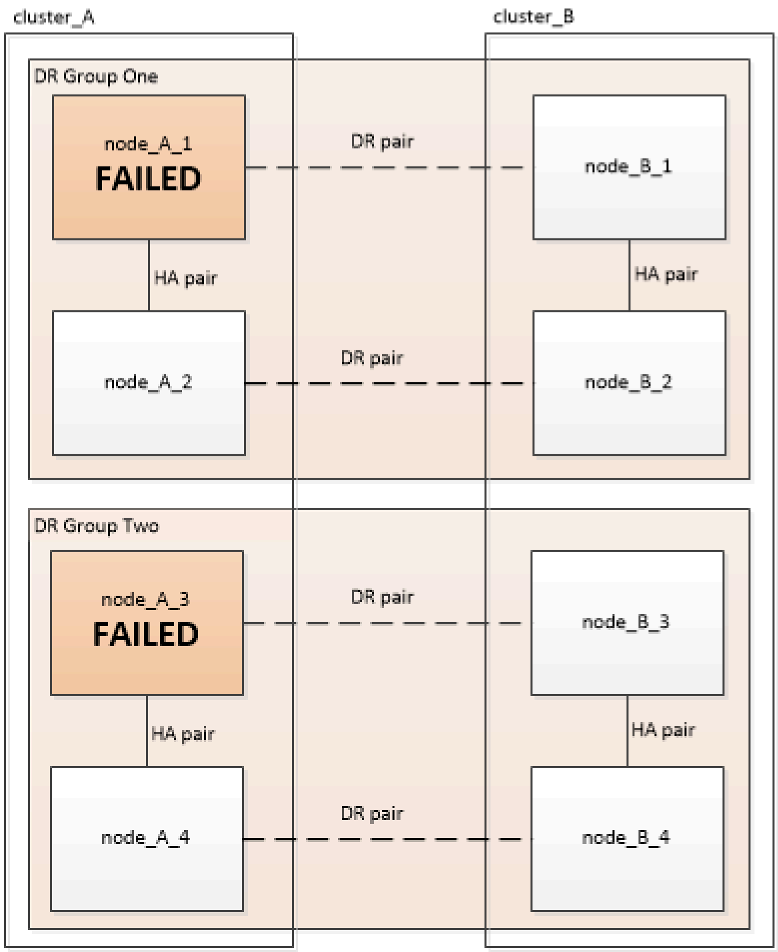
- If no storage requires replacement, you can use the controller module FRU replacement procedure for the platform model.

  The FRU replacement procedure is performed twice, once for each failed controller module.

  AFF and FAS Documentation Center

- If storage requires replacement, you can use the multi-controller module recovery procedure.

  Recovering from a multi-controller or storage failure



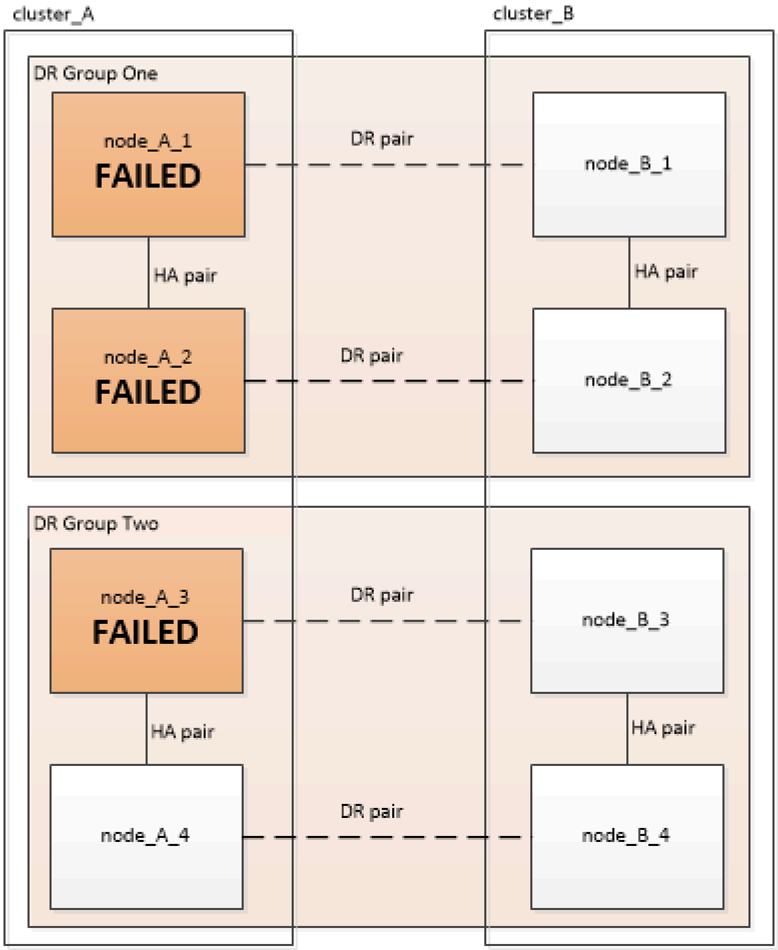
Three controller module failures spread across the DR groups

In this case the failure requires a switchover. You can use the multi-controller module failure recovery procedure for DR Group One.

[Recovering from a multi-controller or storage failure]

You can use the platform-specific controller module FRU replacement procedure for DR Group Two.

[AFF and FAS Documentation Center]



Controller module failure scenarios in two-node MetroCluster configurations

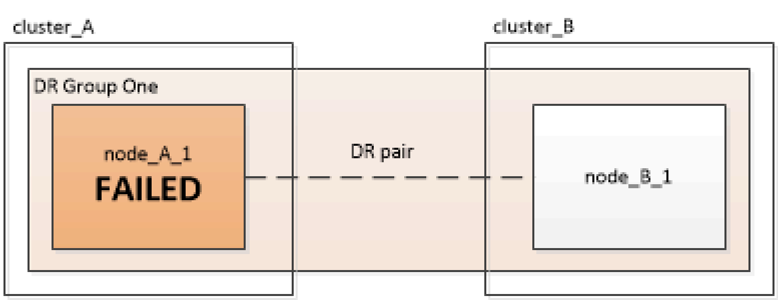
The procedure you use depends on the extent of the failure.

- If no storage requires replacement, you can use the controller module FRU replacement procedure for the platform model.

  AFF and FAS Documentation Center

- If storage requires replacement, you can use the multi-controller module recovery procedure.

  Recovering from a multi-controller or storage failure



Recovering from a multi-controller or storage failure

If the controller failure extends to all controller modules on one side of a DR group in a MetroCluster configuration (including a single controller in a two-node MetroCluster configuration), or storage has been replaced, you must replace the equipment and reassign ownership of drives to recover from the disaster.

Before you begin

- You should review the available recovery procedures before deciding to use this procedure.

  Choosing the correct recovery procedure

- The disaster site must be fenced off.

  Fencing off the disaster site.

- Switchover must have been performed.

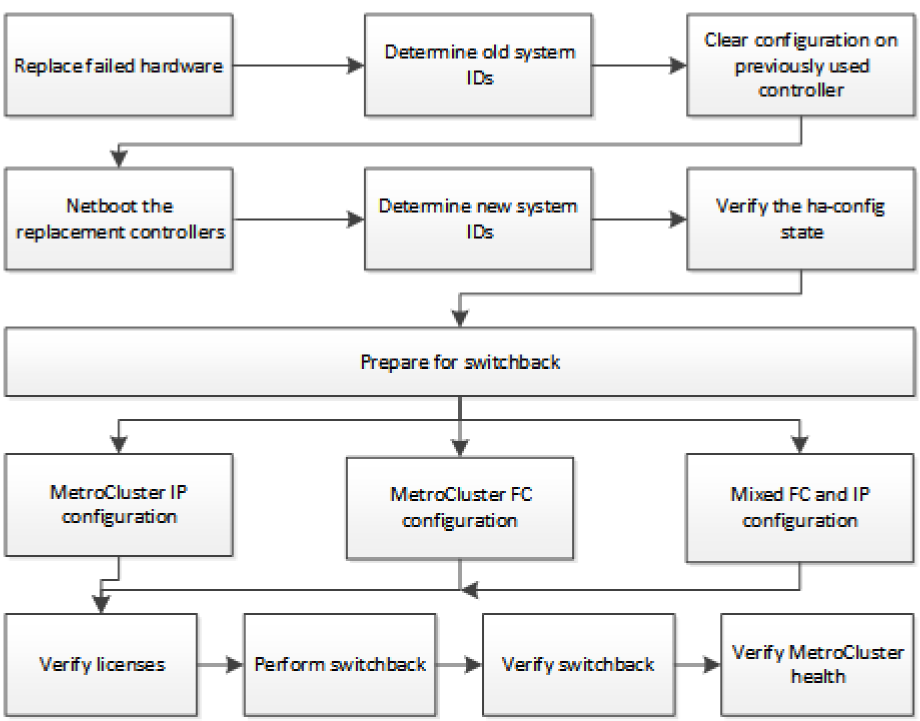
  Performing a forced switchover.

- Replacement drives and the controller modules must be new and must not have been assigned ownership previously.

About this task

The examples in this procedure show two or four-node configurations. If you have an eight-node configuration (two DR groups), you must take into account any failures and perform the required recovery task on the additional controller modules.

This procedure uses the following workflow:



This procedure can be used when performing recovery on a system that was in mid-transition when the failure occurred. In that case, you must perform the appropriate steps when preparing for switchback, as indicated in the procedure.

Replacing hardware and booting new controllers

Replacing hardware at the disaster site

If hardware components have to be replaced, you must replace them using their individual hardware replacement and installation guides.

Before you begin

The storage controllers must be powered off or remain halted (showing the LOADER prompt).

Steps

1. Replace the components as necessary.

> In this step, you replace and cable the components exactly as they were cabled prior to the disaster. You must not power up the components.

If you are replacing…	Perform these steps…	Using these guides…
FC switches in a MetroCluster FC configuration	a. Install the new switches. b. Cable the ISL links. Do not power on the FC switches at this time.	Maintain MetroCluster Components
IP switches in a MetroCluster IP configuration	a. Install the new switches. b. Cable the ISL links. Do not power on the IP switches at this time.	MetroCluster IP installation and configuration
Disk shelves	a. Install the disk shelves and disks. ◦ Disk shelf stacks should be the same configuration as at the surviving site. ◦ Disks can be the same size or larger, but must be of the same type (SAS or SATA). b. Cable the disk shelves to adjacent shelves within the stack and to the FC-to-SAS bridge. Do not power on the disk shelves at this time.	AFF and FAS Documentation Center
SAS cables	a. Install the new cables. Do not power on the disk shelves at this time.	AFF and FAS Documentation Center

FC-to-SAS bridges in a MetroCluster FC configuration	a. Install the FC-to-SAS bridges. b. Cable the FC-to-SAS bridges. Cable them to the FC switches or to the controller modules, depending on your MetroCluster configuration type. Do not power on the FC-to-SAS bridges at this time.	Fabric-attached MetroCluster installation and configuration Stretch MetroCluster installation and configuration

Controller modules	a. Install the new controller modules: ◦ The controller modules must be the same model as those being replaced. For example, 8080 controller modules must be replaced with 8080 controller modules. ◦ The controller modules must not have previously been part of either cluster within the MetroCluster configuration or any previously existing cluster configuration. If they were, you must set defaults and perform a “wipeconfig” process. ◦ Ensure that all network interface cards (such as Ethernet or FC) are in the same slots used on the old controller modules. b. Cable the new controller modules exactly the same as the old ones. The ports connecting the controller module to the storage (either by connections to the IP or FC switches, FC-to-SAS bridges, or directly) should be the same as those used prior to the disaster. Do not power on the controller modules at this time.	AFF and FAS Documentation Center

2. Verify that all components are cabled correctly according to the *MetroCluster Installation and Configuration Guide* for your configuration.

Determining the system IDs and VLAN IDs of the old controller modules

After you have replaced all hardware at the disaster site, you must determine the system IDs of the replaced controller modules. You need the old system IDs when you reassign disks to the new controller modules. If the systems are AFF A220, AFF A250, AFF A400, AFF A800, FAS2750, FAS500f, FAS8300, or FAS8700 models, you must also determine the VLAN IDs used by the MetroCluster IP interfaces.

Before you begin

All equipment at the disaster site must be powered off.

About this task

This discussion provides examples for two and four-node configurations. For eight-node configurations, you must account for any failures in the additional nodes on the second DR group.

For a two-node MetroCluster configuration, you can ignore references to the second controller module at each site.

The examples in this procedure are based on the following assumptions:

- Site A is the disaster site.
- node_A_1 has failed and is being completely replaced.
- node_A_2 has failed and is being completely replaced.

  node _A_2 is present in a four-node MetroCluster configuration only.

- Site B is the surviving site.
- node_B_1 is healthy.
- node_B_2 is healthy.

  node_B_2 is present in a four-node MetroCluster configuration only.

The controller modules have the following original system IDs:

Number of nodes in MetroCluster configuration	Node	Original system ID
Four	node_A_1	4068741258
	node_A_2	4068741260
	node_B_1	4068741254
	node_B_2	4068741256
Two	node_A_1	4068741258
	node_B_1	4068741254

Steps

1. From the surviving site, display the system IDs of the nodes in the MetroCluster configuration.

Number of nodes in MetroCluster configuration	Use this command

Four or eight	`metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`
Two	`metrocluster node show -fields node-systemid,dr-partner-systemid`

In this example for a four-node MetroCluster configuration, the following old system IDs are retrieved:

- Node_A_1: 4068741258
- Node_A_2: 4068741260

  Disks owned by the old controller modules are still owned these system IDs.

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid
dr-partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  4068741258    4068741260
4068741254          4068741256
1           Cluster_A  Node_A_2  4068741260    4068741258
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                   -
-
1           Cluster_B  Node_B_2  -             -                   -
-
4 entries were displayed.
```

In this example for a two-node MetroCluster configuration, the following old system ID is retrieved:

- Node_A_1: 4068741258

  Disks owned by the old controller module are still owned this system ID.

```
metrocluster node show -fields node-systemid,dr-partner-systemid

dr-group-id cluster    node      node-systemid dr-partner-systemid
----------- ---------- --------  ------------- ------------
1           Cluster_A  Node_A_1  4068741258    4068741254
1           Cluster_B  Node_B_1  -             -
2 entries were displayed.
```

2. For MetroCluster IP configurations using the ONTAP Mediator service, get the IP address of the ONTAP Mediator service:

   `storage iscsi-initiator show -node * -label mediator`

3. If the systems are AFF A220, AFF A400, FAS2750, FAS8300, or FAS8700 models, determine the VLAN IDs:

   `metrocluster interconnect show`

   The VLAN IDs are included in the adapter name shown in the Adapter column of the output.

   In this example, the VLAN IDs are 120 and 130:

```
metrocluster interconnect show
                          Mirror   Mirror
                  Partner Admin    Oper
Node Partner Name Type    Status   Status  Adapter Type   Status
---- ------------ ------- -------- ------- ------- ------ ------
Node_A_1 Node_A_2 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
Node_A_2 Node_A_1 HA      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_2 DR      enabled  online
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
         Node_B_1 AUX     enabled  offline
                                           e0a-120 iWARP  Up
                                           e0b-130 iWARP  Up
12 entries were displayed.
```

Isolating replacement drives from the surviving site (MetroCluster IP configurations)

You must isolate any replacement drives by taking down the MetroCluster iSCSI initiator connections from the surviving nodes.

About this task

This procedure is only required on MetroCluster IP configurations.

Steps

1. From either surviving node’s prompt, change to the advanced privilege level:

   `set -privilege advanced`

   You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

2. Disconnect the iSCSI initiators on both surviving nodes in the DR group:

   `storage iscsi-initiator disconnect -node surviving-node -label *`

   This command must be issued twice, once for each of the surviving nodes.

   The following example shows the commands for disconnecting the initiators on site B:

   ```
   site_B::*> storage iscsi-initiator disconnect -node node_B_1 -label *
   site_B::*> storage iscsi-initiator disconnect -node node_B_2 -label *
   ```

3. Return to the admin privilege level:

   `set -privilege admin`

Clearing the configuration on a controller module

Before using a new controller module in the MetroCluster configuration, you must clear the existing configuration.

Steps

1. If necessary, halt the node to display the LOADER prompt:

   `halt`

2. At the LOADER prompt, set the environmental variables to default values:

   `set-defaults`

3. Save the environment:

   `saveenv`

4. At the LOADER prompt, launch the boot menu:

   `boot_ontap menu`

5. At the boot menu prompt, clear the configuration:

   `wipeconfig`

   Respond `yes` to the confirmation prompt.

   The node reboots and the boot menu is displayed again.

6. At the boot menu, select option **5** to boot the system into Maintenance mode.

   Respond `yes` to the confirmation prompt.

Netbooting the new controller modules

If the new controller modules have a different version of ONTAP from the version on the surviving controller modules, you must netboot the new controller modules.

Before you begin

- You must have access to an HTTP server.
- You must have access to the NetApp Support Site to download the necessary system files for your platform and version of ONTAP software that is running on it.

  NetApp Support

Steps

1. Access the NetApp Support Site to download the files used for performing the netboot of the system.
2. Download the appropriate ONTAP software from the software download section of the NetApp Support Site and store the ontap-version_image.tgz file on a web-accessible directory.
3. Go to the web-accessible directory and verify that the files you need are available.

If the platform model is…	Then…
FAS/AFF8000 series systems	Extract the contents of the ontap-version_image.tgzfile to the target directory: tar -zxvf ontap-version_image.tgz NOTE: If you are extracting the contents on Windows, use 7-Zip or WinRAR to extract the netboot image. Your directory listing should contain a netboot folder with a kernel file:netboot/kernel
All other systems	Your directory listing should contain a netboot folder with a kernel file: ontap-version_image.tgz You do not need to extract the ontap-version_image.tgz file.

4. At the LOADER prompt, configure the netboot connection for a management LIF:
   - If IP addressing is DHCP, configure the automatic connection:

     `ifconfig e0M -auto`

   - If IP addressing is static, configure the manual connection:

     `ifconfig e0M -addr=ip_addr -mask=netmask -gw=gateway`

5. Perform the netboot.

◦ If the platform is an 80xx series system, use this command:

`netboot http://web_server_ip/path_to_web-accessible_directory/netboot/kernel`

◦ If the platform is any other system, use the following command:

`netboot http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

6. From the boot menu, select option **(7) Install new software first** to download and install the new software image to the boot device.

```
Disregard the following message: "This procedure is not supported for
Non-Disruptive Upgrade on an HA pair". It applies to nondisruptive
upgrades of software, not to upgrades of controllers.
```

7. If you are prompted to continue the procedure, enter `y`, and when prompted for the package, enter the URL of the image file: `http://web_server_ip/path_to_web-accessible_directory/ontap-version_image.tgz`

```
Enter username/password if applicable, or press Enter to continue.
```

8. Be sure to enter `n` to skip the backup recovery when you see a prompt similar to the following:

```
Do you want to restore the backup configuration now? {y|n}
```

9. Reboot by entering `y` when you see a prompt similar to the following:

```
The node must be rebooted to start using the newly installed software.
Do you want to reboot now? {y|n}
```

10. From the Boot menu, select **option 5** to enter Maintenance mode.
11. If you have a four-node MetroCluster configuration, repeat this procedure on the other new controller module.

Determining the system IDs of the replacement controller modules

After you have replaced all hardware at the disaster site, you must determine the system ID of the newly installed storage controller module or modules.

About this task

You must perform this procedure with the replacement controller modules in Maintenance mode.

This section provides examples for two and four-node configurations. For two-node configurations, you can ignore references to the second node at each site. For eight-node configurations, you must account for the additional nodes on the second DR group. The examples make the following assumptions:

- Site A is the disaster site.
- node_A_1 has been replaced.
- node_A_2 has been replaced.

  Present only in four-node MetroCluster configurations.

- Site B is the surviving site.
- node_B_1 is healthy.
- node_B_2 is healthy.

  Present only in four-node MetroCluster configurations.

The examples in this procedure use controllers with the following system IDs:

Number of nodes in MetroCluster configuration	Node	Original system ID	New system ID	Will pair with this node as DR partner
Four	node_A_1	4068741258	1574774970	node_B_1
	node_A_2	4068741260	1574774991	node_B_2
	node_B_1	4068741254	unchanged	node_A_1
	node_B_2	4068741256	unchanged	node_A_2
Two	node_A_1	4068741258	1574774970	node_B_1
	node_B_1	4068741254	unchanged	node_A_1

In a four-node MetroCluster configuration, the system determines DR partnerships by pairing the node with the lowest system ID at site_A and the node with the lowest system ID at site_B. Because the system IDs change, the DR pairs might be different after the controller replacements are completed than they were prior to the disaster.

In the preceding example:

- node_A_1 (1574774970) will be paired with node_B_1 (4068741254)
- node_A_2 (1574774991) will be paired with node_B_2 (4068741256)

Steps

1. With the node in Maintenance mode, display the local system ID of the node from each node: `disk show`

   In the following example, the new local system ID is 1574774970:

```
*> disk show
 Local System ID: 1574774970
 ...
```

2. On the second node, repeat the previous step.

   This step is not required in a two-node MetroCluster configuration.

   In the following example, the new local system ID is 1574774991:

```
*> disk show
 Local System ID: 1574774991
 ...
```

Verifying the ha-config state of components

In a MetroCluster configuration, the ha-config state of the controller module and chassis components must be set to "mcc" or "mcc-2n" so they boot up properly.

Before you begin

The system must be in Maintenance mode.

About this task

This task must be performed on each new controller module.

Steps

1. In Maintenance mode, display the HA state of the controller module and chassis:

   `ha-config show`

   The correct HA state depends on your MetroCluster configuration.

Number of controllers in the MetroCluster configuration	HA state for all components should be…
Eight- or four-node MetroCluster FC configuration	mcc
Two-node MetroCluster FC configuration	mcc-2n
MetroCluster IP configuration	mccip

2. If the displayed system state of the controller is not correct, set the HA state for the controller module:

Number of controllers in the MetroCluster configuration	Command

Eight- or four-node MetroCluster FC configuration	`ha-config modify controller mcc`
Two-node MetroCluster FC configuration	`ha-config modify controller mcc-2n`
MetroCluster IP configuration	`ha-config modify controller mccip`

3. If the displayed system state of the chassis is not correct, set the HA state for the chassis:

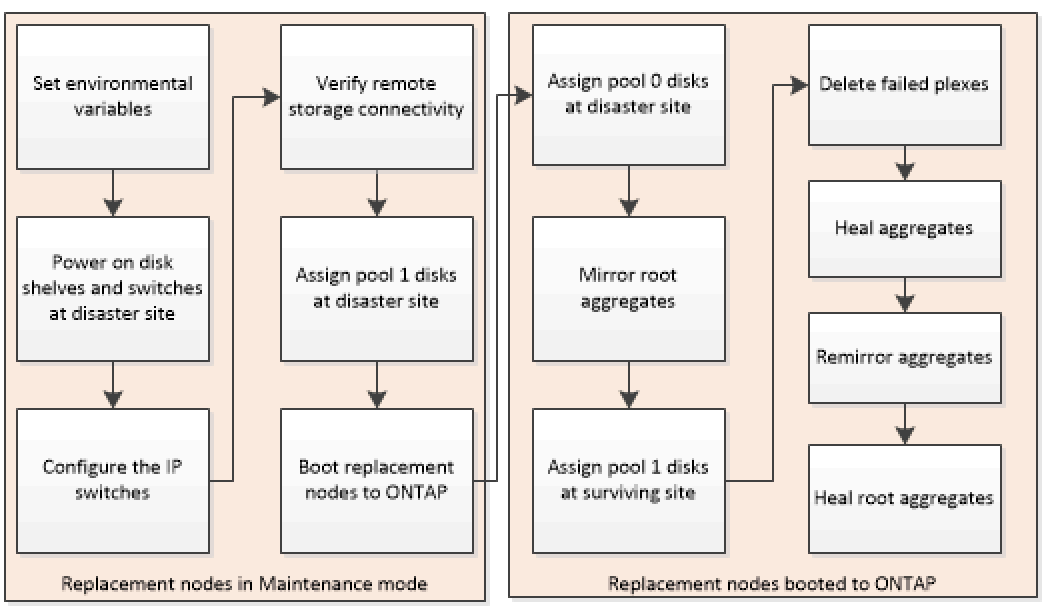
Number of controllers in the MetroCluster configuration	**Command**
Eight- or four-node MetroCluster FC configuration	`ha-config modify chassis mcc`
Two-node MetroCluster FC configuration	`ha-config modify chassis mcc-2n`
MetroCluster IP configuration	`ha-config modify chassis mccip`

4. Repeat these steps on the other replacement node.

Prepare for switchback in a MetroCluster IP configuration

You must perform certain tasks in order to prepare the MetroCluster IP configuration for the switchback operation.

About this task



Setting required environmental variables in MetroCluster IP configurations

In MetroCluster IP configurations, you must retrieve the IP address of the MetroCluster interfaces on the Ethernet ports, and then use them to configure the interfaces on the replacement controller modules.

About this task

This task is required only in MetroCluster IP configurations.

Commands in this task are performed from the cluster prompt of the surviving site and from the LOADER prompt of the nodes at the disaster site.

The nodes in these examples have the following IP addresses for their MetroCluster IP connections:

These examples are for an AFF A700 or FAS9000 system. The interfaces vary by platform model.

Node	Port	IP address
node_A_1	e5a	172.17.26.10
e5b	172.17.27.10	node_A_2
e5a	172.17.26.11	e5b
172.17.27.11	node_B_1	e5a
172.17.26.13	e5b	172.17.27.13
node_B_2	e5a	172.17.26.12

The following table summarizes the relationships between the nodes and each node's MetroCluster IP addresses.

Node	HA partner	DR partner	DR auxiliary partner
node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11	node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13	node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12
node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11	node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12	node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13
node_B_1 • e5a: 172.17.26.13 • e5b: 172.17.27.13	node_B_2 • e5a: 172.17.26.12 • e5b: 172.17.27.12	node_A_1 • e5a: 172.17.26.10 • e5b: 172.17.27.10	node_A_2 • e5a: 172.17.26.11 • e5b: 172.17.27.11

node_B_2	node_B_1	node_A_2	node_A_1
• e5a: 172.17.26.12 • e5b: 172.17.27.12	• e5a: 172.17.26.13 • e5b: 172.17.27.13	• e5a: 172.17.26.11 • e5b: 172.17.27.11	• e5a: 172.17.26.10 • e5b: 172.17.27.10

The following table lists the platform models that use VLAN IDs on the MetroCluster IP interfaces. These models might require additional steps if you are not using the default VLAN IDs.

Platform models that use VLAN IDs with the MetroCluster IP interfaces	
• AFF A220 • AFF A250 • AFF A400	• FAS500f • FAS2750 • FAS8300 • FAS8700

Steps

1. From the surviving site, gather the IP addresses of the MetroCluster interfaces on the disaster site:

   `metrocluster configuration-settings connection show`

   The required addresses are the DR Partner addresses shown in the **Destination Network Address** column.

   The following output shows the IP addresses for a configuration with AFF A700 and FAS9000 systems with the MetroCluster IP interfaces on ports e5a and e5b. The interfaces vary depending on platform type.

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_1
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.12    HA Partner
```

```
completed
                    Home Port: e5b
                        172.17.27.13    172.17.27.10    DR Partner
completed
                    Home Port: e5b
                        172.17.27.13    172.17.27.11    DR Auxiliary
completed
                 node_B_2
                    Home Port: e5a
                        172.17.26.12    172.17.26.13    HA Partner
completed
                    Home Port: e5a
                        172.17.26.12    172.17.26.11    DR Partner
completed
                    Home Port: e5a
                        172.17.26.12    172.17.26.10    DR Auxiliary
completed
                    Home Port: e5b
                        172.17.27.12    172.17.27.13    HA Partner
completed
                    Home Port: e5b
                        172.17.27.12    172.17.27.11    DR Partner
completed
                    Home Port: e5b
                        172.17.27.12    172.17.27.10    DR Auxiliary
completed
12 entries were displayed.
```

2. If you need to determine the VLAN ID or gateway address for the interface, determine the VLAN IDs from the surviving site:

   `metrocluster configuration-settings interface show`

   - You need the VLAN ID if the platform models use VLAN IDs (see the list above), and if you are not using the default VLAN IDs.
   - You need the gateway address if you are using Layer 3 wide-area networks.

     The VLAN IDs are included in the **Network Address** column of the output. The **Gateway** column shows the gateway IP address.

     In this example the interfaces are e0a with the VLAN ID 120 and e0b with the VLAN ID 130:

```
Cluster-A::*> metrocluster configuration-settings interface show
DR
Config
Group Cluster Node     Network Address Netmask         Gateway
State
----- ------- ------- --------------- --------------- ---------------
---------
1
      cluster_A
              node_A_1
                  Home Port: e0a-120
                          172.17.26.10  255.255.255.0  -
completed
                  Home Port: e0b-130
                          172.17.27.10  255.255.255.0  -
completed
```

3. If the disaster site nodes use VLAN IDs (see the list above), at the LOADER prompt for each of the disaster site nodes, set the following bootargs:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-
mask,gateway-IP-address,HA-partner-IP-address,DR-partner-IP-address,DR-
aux-partnerIP-address,vlan-id

setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-
mask,gateway-IP-address,HA-partner-IP-address,DR-partner-IP-address,DR-
aux-partnerIP-address,vlan-id
```

> ◦ If the interfaces are using the default VLANs, or the platform model does not require a VLAN (see the list above), the *vlan-id* is not necessary.
>
> ◦ If the configuration is not using Layer3 wide-area networks, the value for *gateway-IP-address* is **0** (zero).

◦ If the interfaces are using the default VLANs, or the platform model does not require a VLAN (see the list above), the *vlan-id* is not necessary.

◦ If the configuration is not using layer 3 backend connections, the value for *gateway-IP-address* is **0** (zero).

The following commands set the values for node_A_1 using VLAN 120 for the first network and VLAN 130 for the second network:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12,120

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12,130
```

The following example shows the commands for node_A_1 without a VLAN ID:

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

4. If the disaster site nodes are not systems that use VLAN IDs, at the LOADER prompt for each of the disaster nodes, set the following bootargs with local_IP/mask,gateway:

```
setenv bootarg.mcc.port_a_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address


setenv bootarg.mcc.port_b_ip_config local-IP-address/local-IP-mask,0,HA-
partner-IP-address,DR-partner-IP-address,DR-aux-partnerIP-address
```

- If the interfaces are using the default VLANs, or the platform model does not require a VLAN (see the list above), the *vlan-id* is not necessary.
- If the configuration is not using Layer 3 wide-area networks, the value for *gateway-IP-address* is **0** (zero).

The following commands set the values for node_A_1. In this example, the *gateway-IP-address* and *vlan-id* values are not used.

```
setenv bootarg.mcc.port_a_ip_config
172.17.26.10/23,0,172.17.26.11,172.17.26.13,172.17.26.12

setenv bootarg.mcc.port_b_ip_config
172.17.27.10/23,0,172.17.27.11,172.17.27.13,172.17.27.12
```

5. From the surviving site, gather the UUIDs for the disaster site:

```
metrocluster node show -fields node-cluster-uuid, node-uuid
```

```
cluster_B::> metrocluster node show -fields node-cluster-uuid, node-uuid

  (metrocluster node show)
dr-group-id cluster     node     node-uuid
node-cluster-uuid
----------- ----------- -------- ------------------------------------
------------------------------
1           cluster_A   node_A_1 f03cb63c-9a7e-11e7-b68b-00a098908039
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_A   node_A_2 aa9a7a7a-9a81-11e7-a4e9-00a098908c35
ee7db9d5-9a82-11e7-b68b-00a098

908039
1           cluster_B   node_B_1 f37b240b-9ac1-11e7-9b42-00a098c9e55d
07958819-9ac6-11e7-9b42-00a098

c9e55d
1           cluster_B   node_B_2 bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
07958819-9ac6-11e7-9b42-00a098

c9e55d
4 entries were displayed.
cluster_A::*>
```

Node	UUID
cluster_B	07958819-9ac6-11e7-9b42-00a098c9e55d
node_B_1	f37b240b-9ac1-11e7-9b42-00a098c9e55d
node_B_2	bf8e3f8f-9ac4-11e7-bd4e-00a098ca379f
cluster_A	ee7db9d5-9a82-11e7-b68b-00a098908039
node_A_1	f03cb63c-9a7e-11e7-b68b-00a098908039
node_A_2	aa9a7a7a-9a81-11e7-a4e9-00a098908c35

6. At the replacement nodes' LOADER prompt, set the UUIDs:

```
setenv bootarg.mgwd.partner_cluster_uuid partner-cluster-UUID

setenv bootarg.mgwd.cluster_uuid local-cluster-UUID

setenv bootarg.mcc.pri_partner_uuid DR-partner-node-UUID

setenv bootarg.mcc.aux_partner_uuid DR-aux-partner-node-UUID

setenv bootarg.mcc_iscsi.node_uuid local-node-UUID`
```

a. Set the UUIDs on node_A_1.

   The following example shows the commands for setting the UUIDs on node_A_1:

   ```
   setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

   setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
   00a098c9e55d

   setenv bootarg.mcc.pri_partner_uuid f37b240b-9ac1-11e7-9b42-
   00a098c9e55d

   setenv bootarg.mcc.aux_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
   00a098ca379f

   setenv bootarg.mcc_iscsi.node_uuid f03cb63c-9a7e-11e7-b68b-
   00a098908039
   ```

b. Set the UUIDs on node_A_2:

   The following example shows the commands for setting the UUIDs on node_A_2:

```
setenv bootarg.mgwd.cluster_uuid ee7db9d5-9a82-11e7-b68b-00a098908039

setenv bootarg.mgwd.partner_cluster_uuid 07958819-9ac6-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc.pri_partner_uuid bf8e3f8f-9ac4-11e7-bd4e-
00a098ca379f

setenv bootarg.mcc.aux_partner_uuid f37b240b-9ac1-11e7-9b42-
00a098c9e55d

setenv bootarg.mcc_iscsi.node_uuid aa9a7a7a-9a81-11e7-a4e9-
00a098908c35
```

7. If the original systems were configured for ADP, at each of the replacement nodes' LOADER prompt, enable ADP:

   `setenv bootarg.mcc.adp_enabled true`

8. If running ONTAP 9.5, 9.6 or 9.7, at each of the replacement nodes' LOADER prompt, enable the following variable:

   `setenv bootarg.mcc.lun_part true`

   a. Set the variables on node_A_1.

      The following example shows the commands for setting the values on node_A_1 when running ONTAP 9.6:

      ```
      setenv bootarg.mcc.lun_part true
      ```

   b. Set the variables on node_A_2.

      The following example shows the commands for setting the values on node_A_2 when running ONTAP 9.6:

      ```
      setenv bootarg.mcc.lun_part true
      ```

9. If the original systems were configured for ADP, at each of the replacement nodes' LOADER prompt, set the original system ID (**not** the system ID of the replacement controller module) and the system ID of the DR partner of the node:

   `setenv bootarg.mcc.local_config_id original-sysID`

   `setenv bootarg.mcc.dr_partner dr_partner-sysID`

   Determining the system IDs and VLAN IDs of the old controller modules

a. Set the variables on node_A_1.

   The following example shows the commands for setting the system IDs on node_A_1:

   - The old system ID of node_A_1 is 4068741258.
   - The system ID of node_B_1 is 4068741254.

   ```
   setenv bootarg.mcc.local_config_id 4068741258
   setenv bootarg.mcc.dr_partner 4068741254
   ```

b. Set the variables on node_A_2.

   The following example shows the commands for setting the system IDs on node_A_2:

   - The old system ID of node_A_1 is 4068741260.
   - The system ID of node_B_1 is 4068741256.

   ```
   setenv bootarg.mcc.local_config_id 4068741260
   setenv bootarg.mcc.dr_partner 4068741256
   ```

Powering on the equipment at the disaster site (MetroCluster IP configurations)

You must power on the disk shelves and MetroCluster IP switches components at the disaster site. The controller modules at the disaster site remain at the LOADER prompt.

About this task

The examples in this procedure assume the following:

- Site A is the disaster site.
- Site B is the surviving site.

Steps

1. Turn on the disk shelves at the disaster site and make sure that all disks are running.
2. Turn on the MetroCluster IP switches if they are not already on.

Configuring the IP switches (MetroCluster IP configurations)

You must configure any IP switches that were replaced.

About this task

This task applies to MetroCluster IP configurations only.

This must be done on both switches. Verify after configuring the first switch that storage access on the surviving site is not impacted.

> You must not proceed with the second switch if storage access on the surviving site is impacted.

Steps

1. Refer to MetroCluster IP installation and configuration for procedures for cabling and configuring a replacement switch.

   You can use the procedures in the following sections:

   - Cabling the IP switches
   - Configuring the IP switches

2. If the ISLs were disabled at the surviving site, enable the ISLs and verify that the ISLs are online.

   a. Enable the ISL interfaces on the first switch:

   `no shutdown`

   The following examples show the commands for a Broadcom IP switch or a Cisco IP switch.

Switch vendor	Commands

Broadcom	`(IP_Switch_A_1)> enable`
	`(IP_switch_A_1)# configure`
	`(IP_switch_A_1)(Config)# interface 0/13-0/16`
	`(IP_switch_A_1)(Interface 0/13-0/16 )# no shutdown`
	`(IP_switch_A_1)(Interface 0/13-0/16 )# exit`
	`(IP_switch_A_1)(Config)# exit`

Cisco	`IP_switch_A_1# conf t`
	`IP_switch_A_1(config)# int eth1/15-eth1/20`
	`IP_switch_A_1(config)# no shutdown`
	`IP_switch_A_1(config)# copy running startup`
	`IP_switch_A_1(config)# show interface brief`

   b. Enable the ISL interfaces on the partner switch:

   `no shutdown`

   The following examples show the commands for a Broadcom IP switch or a Cisco IP switch.

Switch vendor	Commands

Broadcom	```(IP_Switch_A_2)> enable```
	```(IP_switch_A_2)# configure```
	```(IP_switch_A_2)(Config)# interface 0/13-0/16```
	```(IP_switch_A_2)(Interface 0/13-0/16)# no shutdown```
	```(IP_switch_A_2)(Interface 0/13-0/16)# exit```
	```(IP_switch_A_2)(Config)# exit```

Cisco	```IP_switch_A_2# conf t```
	```IP_switch_A_2(config)# int eth1/15-eth1/20```
	```IP_switch_A_2(config)# no shutdown```
	```IP_switch_A_2(config)# copy running startup```
	```IP_switch_A_2(config)# show interface brief```

c. Verify that the interfaces are enabled:

```
show interface brief
```

The following example shows the output for a Cisco switch.

```
IP_switch_A_2(config)# show interface brief

--------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------
mt0 -- up 10.10.99.10 100 1500
--------------------------------------------------------
Ethernet    VLAN Type Mode    Status Reason Speed   Port
Interface                                           Ch
#
--------------------------------------------------------
.
.
.
Eth1/15    10   eth   access  up     none   40G(D)  --
Eth1/16    10   eth   access  up     none   40G(D)  --
Eth1/17    10   eth   access  down   none   auto(D) --
Eth1/18    10   eth   access  down   none   auto(D) --
Eth1/19    10   eth   access  down   none   auto(D) --
Eth1/20    10   eth   access  down   none   auto(D) --
.
.
.
IP_switch_A_2#
```

Verify storage connectivity to the remote site (MetroCluster IP configurations)

You must confirm that the replaced nodes have connectivity to the disk shelves at the surviving site.

About this task

This task is performed on the replacement nodes at the disaster site.

This task is performed in Maintenance mode.

Steps

1. Display the disks that are owned by the original system ID.

   `disk show -s old-system-ID`

   The remote disks can be recognized by the 0m device. 0m indicates that the disk is connected via the MetroCluster iSCSI connection. These disks must be reassigned later in the recovery procedure.

```
*> disk show -s 4068741256
Local System ID: 1574774970

  DISK      OWNER                   POOL   SERIAL NUMBER    HOME
DR HOME
---------- --------------------- ----- -------------
--------------------- ----------------------
0m.i0.0L11 node_A_2 (4068741256) Pool1 S396NA0HA02128  node_A_2
(4068741256) node_A_2  (4068741256)
0m.i0.1L38 node_A_2 (4068741256) Pool1 S396NA0J148778  node_A_2
(4068741256) node_A_2  (4068741256)
0m.i0.0L52 node_A_2 (4068741256) Pool1 S396NA0J148777  node_A_2
(4068741256) node_A_2  (4068741256)
...
...
NOTE: Currently 49 disks are unowned. Use 'disk show -n' for additional
information.
*>
```

2. Repeat this step on the other replacement nodes

Reassigning disk ownership for pool 1 disks on the disaster site (MetroCluster IP configurations)

If one or both of the controller modules or NVRAM cards were replaced at the disaster site, the system ID has changed and you must reassign disks belonging to the root aggregates to the replacement controller modules.

About this task

Because the nodes are in switchover mode, only the disks containing the root aggregates of pool1 of the disaster site will be reassigned in this task. They are the only disks still owned by the old system ID at this point.

This task is performed on the replacement nodes at the disaster site.

This task is performed in Maintenance mode.

The examples make the following assumptions:

- Site A is the disaster site.
- node_A_1 has been replaced.
- node_A_2 has been replaced.
- Site B is the surviving site.
- node_B_1 is healthy.
- node_B_2 is healthy.

The old and new system IDs were identified in Determining the new System IDs of the replacement controller modules.

The examples in this procedure use controllers with the following system IDs:

Node	Original system ID	New system ID
node_A_1	4068741258	1574774970
node_A_2	4068741260	1574774991
node_B_1	4068741254	unchanged
node_B_2	4068741256	unchanged

Steps

1. With the replacement node in Maintenance mode, reassign the root aggregate disks, using the correct command, depending on whether your system is configured with ADP and your ONTAP version.

   You can proceed with the reassignment when prompted.

If the system is using ADP…	Use this command for disk reassignment…
Yes (ONTAP 9.8)	`disk reassign -s old-system-ID -d new-system-ID -r dr-partner-system-ID`
Yes (ONTAP 9.7.x and earlier)	`disk reassign -s old-system-ID -d new-system-ID -p old-partner-system-ID`
No	`disk reassign -s old-system-ID -d new-system-ID`

   The following example shows reassignment of drives on a non-ADP system:

```
*> disk reassign -s 4068741256 -d 1574774970
Partner node must not be in Takeover mode during disk reassignment from
maintenance mode.
Serious problems could result!!
Do not proceed with reassignment if the partner is in takeover mode.
Abort reassignment (y/n)? n

After the node becomes operational, you must perform a takeover and
giveback of the HA partner node to ensure disk reassignment is
successful.
Do you want to continue (y/n)? y
Disk ownership will be updated on all disks previously belonging to
Filer with sysid 537037643.
Do you want to continue (y/n)? y
disk reassign parameters: new_home_owner_id 537070473 ,
new_home_owner_name
Disk 0m.i0.3L14 will be reassigned.
Disk 0m.i0.1L6 will be reassigned.
Disk 0m.i0.1L8 will be reassigned.
Number of disks to be reassigned: 3
```

2. Destroy the contents of the mailbox disks:

   `mailbox destroy local`

   You can proceed with the destroy operation when prompted.

   The following example shows the output for the mailbox destroy local command:

```
*> mailbox destroy local
Destroying mailboxes forces a node to create new empty mailboxes,
which clears any takeover state, removes all knowledge
of out-of-date plexes of mirrored volumes, and will prevent
management services from going online in 2-node cluster
HA configurations.
Are you sure you want to destroy the local mailboxes? y
...............Mailboxes destroyed.
*>
```

3. If disks have been replaced, there will be failed local plexes that must be deleted.
   a. Display the aggregate status:

      `aggr status`

      In the following example, plex node_A_1_aggr0/plex0 has failed.

```
*> aggr status
Aug 18 15:00:07 [node_B_1:raid.vol.mirror.degraded:ALERT]: Aggregate
node_A_1_aggr0 is
   mirrored and one plex has failed. It is no longer protected by
mirroring.
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
node_A_1_aggr0 has plex0
   clean(-1), online(0)
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Mirrored aggregate
node_A_1_aggr0 has plex2
   clean(0), online(1)
Aug 18 15:00:07 [node_B_1:raid.mirror.vote.noRecord1Plex:error]:
WARNING: Only one plex
   in aggregate node_A_1_aggr0 is available. Aggregate might contain
stale data.
Aug 18 15:00:07 [node_B_1:raid.debug:info]:
volobj_mark_sb_recovery_aggrs: tree:
   node_A_1_aggr0 vol_state:1 mcc_dr_opstate: unknown
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0 (VOL):
   raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0 (MIRROR):
   raid state change UNINITD -> DEGRADED
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex0
   (PLEX): raid state change UNINITD -> FAILED
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex2
   (PLEX): raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.fsm.commitStateTransit:debug]:
/node_A_1_aggr0/plex2/rg0
   (GROUP): raid state change UNINITD -> NORMAL
Aug 18 15:00:07 [node_B_1:raid.debug:info]: Topology updated for
aggregate node_A_1_aggr0
   to plex plex2
*>
```

b. Delete the failed plex:

`aggr destroy plex-id`

```
*> aggr destroy node_A_1_aggr0/plex0
```

4. Halt the node to display the LOADER prompt:

   `halt`

5. Repeat these steps on the other node at the disaster site.

Booting to ONTAP on replacement controller modules in MetroCluster IP configurations

You must boot the replacement nodes at the disaster site to the ONTAP operating system.

About this task

This task begins with the nodes at the disaster site in Maintenance mode.

Steps

1. On one of the replacement nodes, exit to the LOADER prompt: `halt`
2. Display the boot menu: `boot_ontap menu`
3. From the boot menu, select option 6, **Update flash from backup config**.

   The system boots twice. You should respond `yes` when prompted to continue. After the second boot, you should respond `y` when prompted about the system ID mismatch.

   > If you did not clear the NVRAM contents of a used replacement controller module, then you might see the following panic message: `PANIC: NVRAM contents are invalid...`. If this occurs, boot the system to the ONTAP prompt again (`boot_ontap menu`). You then need to perform a root recovery. Contact technical support for assistance.

   - Confirmation to continue prompt:

     ```
     Selection (1-9)? 6

     This will replace all flash-based configuration with the last backup
     to
     disks. Are you sure you want to continue?: yes
     ```

   - System ID mismatch prompt:

     ```
     WARNING: System ID mismatch. This usually occurs when replacing a
     boot device or NVRAM cards!
     Override system ID? {y|n} y
     ```

4. From the surviving site, verify that the correct partner system IDs have been applied to the nodes:

   `metrocluster node show -fields node-systemid,ha-partner-systemid,dr-partner-systemid,dr-auxiliary-systemid`

   In this example, the following new system IDs should appear in the output:

- Node_A_1: 1574774970
- Node_A_2: 1574774991

The "ha-partner-systemid" column should show the new system IDs.

```
metrocluster node show -fields node-systemid,ha-partner-systemid,dr-
partner-systemid,dr-auxiliary-systemid

dr-group-id cluster    node      node-systemid ha-partner-systemid dr-
partner-systemid dr-auxiliary-systemid
----------- ---------- --------  ------------- ------ ------------
------ ------------ ------ --------------
1           Cluster_A  Node_A_1  1574774970    1574774991
4068741254          4068741256
1           Cluster_A  Node_A_2  1574774991    1574774970
4068741256          4068741254
1           Cluster_B  Node_B_1  -             -                   -
-
1           Cluster_B  Node_B_2  -             -                   -
-
4 entries were displayed.
```

5. If the partner system IDs were not correctly set, you must manually set the correct value:
   a. Halt and display the LOADER prompt on the node.
   b. Verify the partner-sysID bootarg's current value:

      `printenv`

   c. Set the value to the correct partner system ID:

      `setenv partner-sysid partner-sysID`

   d. Boot the node:

      `boot_ontap`

   e. Repeat these substeps on the other node, if necessary.
6. Confirm that the replacement nodes at the disaster site are ready for switchback:

   `metrocluster node show`

   The replacement nodes should be in waiting for switchback recovery mode. If they are in normal mode instead, you can reboot the replacement nodes. After that boot, the nodes should be in waiting for switchback recovery mode.

   The following example shows that the replacement nodes are ready for switchback:

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   switchover
completed
              node_B_2           configured     enabled   switchover
completed
      cluster_A
              node_A_1           configured     enabled   waiting for
switchback recovery
              node_A_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

7. Verify the MetroCluster connection configuration settings:

`metrocluster configuration-settings connection show`

The configuration state should indicate completed.

```
cluster_B::*> metrocluster configuration-settings connection show
DR                    Source          Destination
Group Cluster Node    Network Address Network Address Partner Type
Config State
----- ------- ------- --------------- --------------- ------------
------------
1     cluster_B
              node_B_2
                 Home Port: e5a
                      172.17.26.13    172.17.26.12    HA Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.10    DR Partner
completed
                 Home Port: e5a
                      172.17.26.13    172.17.26.11    DR Auxiliary
completed
                 Home Port: e5b
                      172.17.27.13    172.17.27.12    HA Partner
completed
```

```
                Home Port: e5b
                     172.17.27.13    172.17.27.10    DR Partner
completed
                Home Port: e5b
                     172.17.27.13    172.17.27.11    DR Auxiliary
completed
             node_B_1
                Home Port: e5a
                     172.17.26.12    172.17.26.13    HA Partner
completed
                Home Port: e5a
                     172.17.26.12    172.17.26.11    DR Partner
completed
                Home Port: e5a
                     172.17.26.12    172.17.26.10    DR Auxiliary
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.13    HA Partner
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.11    DR Partner
completed
                Home Port: e5b
                     172.17.27.12    172.17.27.10    DR Auxiliary
completed
     cluster_A
             node_A_2
                Home Port: e5a
                     172.17.26.11    172.17.26.10    HA Partner
completed
                Home Port: e5a
                     172.17.26.11    172.17.26.12    DR Partner
completed
                Home Port: e5a
                     172.17.26.11    172.17.26.13    DR Auxiliary
completed
                Home Port: e5b
                     172.17.27.11    172.17.27.10    HA Partner
completed
                Home Port: e5b
                     172.17.27.11    172.17.27.12    DR Partner
completed
                Home Port: e5b
                     172.17.27.11    172.17.27.13    DR Auxiliary
completed
             node_A_1
```

```
                  Home Port: e5a
                       172.17.26.10    172.17.26.11    HA Partner
completed
                  Home Port: e5a
                       172.17.26.10    172.17.26.13    DR Partner
completed
                  Home Port: e5a
                       172.17.26.10    172.17.26.12    DR Auxiliary
completed
                  Home Port: e5b
                       172.17.27.10    172.17.27.11    HA Partner
completed
                  Home Port: e5b
                       172.17.27.10    172.17.27.13    DR Partner
completed
                  Home Port: e5b
                       172.17.27.10    172.17.27.12    DR Auxiliary
completed
24 entries were displayed.

cluster_B::*>
```

8. Repeat the previous steps on the other node at the disaster site.

Restoring connectivity from the surviving nodes to the disaster site (MetroCluster IP configurations)

You must restore the MetroCluster iSCSI initiator connections from the surviving nodes.

About this task

This procedure is only required on MetroCluster IP configurations.

Steps

1. From either surviving node's prompt, change to the advanced privilege level:

   `set -privilege advanced`

   You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

2. Connect the iSCSI initiators on both surviving nodes in the DR group:

   `storage iscsi-initiator connect -node surviving-node -label *`

   The following example shows the commands for connecting the initiators on site B:

```
site_B::*> storage iscsi-initiator connect -node node_B_1 -label *
site_B::*> storage iscsi-initiator connect -node node_B_2 -label *
```

3. Return to the admin privilege level:

```
set -privilege admin
```

Verifying automatic assignment or manually assigning pool 0 drives

On systems configured for ADP, you must verify that pool 0 drives have been automatically assigned. On systems that are not configured for ADP, you must manually assign the pool 0 drives.

Verifying drive assignment of pool 0 drives on ADP systems at the disaster site (MetroCluster IP systems)

If drives have been replaced at the disaster site and the system is configured for ADP, you must verify that the remote drives are visible to the nodes and have been assigned correctly.

Step

1. Verify that pool 0 drives are assigned automatically:

```
disk show
```

In the following example for an AFF A800 system with no external shelves, one quarter (8 drives) were automatically assigned to node_A_1 and one quarter were automatically assigned to node_A_2. The remaining drives will be remote (pool1) drives for node_B_1 and node_B_2.

```
cluster_A::*> disk show
                 Usable     Disk      Container           Container
Disk             Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_A_1
node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_A_1
node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
```

```
node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

Assigning pool 0 drives on non-ADP systems at the disaster site (MetroCluster IP configurations)

If drives have been replaced at the disaster site and the system is not configured for ADP, you need to manually assign new drives to pool 0.

About this task

For ADP systems, the drives are assigned automatically.

Steps

1. On one of the replacement nodes at the disaster site, reassign the node’s pool 0 drives:

   ```
   storage disk assign -n number-of-replacement disks -p 0
   ```

   This command assigns the newly added (and unowned) drives on the disaster site. You should assign the same number and size (or larger) of drives that the node had prior to the disaster. The `storage disk` `assign` man page contains more information about performing more granular drive assignment.

2. Repeat the step on the other replacement node at the disaster site.

Assigning pool 1 drives on the surviving site (MetroCluster IP configurations)

If drives have been replaced at the disaster site and the system is not configured for ADP, at the surviving site you need to manually assign remote drives located at the disaster site to the surviving nodes' pool 1. You must identify the number of drives to assign.

About this task

For ADP systems, the drives are assigned automatically.

Step

1. On the surviving site, assign the first node's pool 1 (remote) drives: `storage disk assign -n number-of-replacement disks -p 1 0m*`

   This command assigns the newly added and unowned drives on the disaster site.

   The following command assigns 22 drives:

   ```
   cluster_B::> storage disk assign -n 22 -p 1 0m*
   ```

Deleting failed plexes owned by the surviving site (MetroCluster IP configurations)

After replacing hardware and assigning disks, you must delete failed remote plexes that are owned by the surviving site nodes but located at the disaster site.

About this task

These steps are performed on the surviving cluster.

Steps

1. Identify the local aggregates: `storage aggregate show -is-home true`

   ```
   cluster_B::> storage aggregate show -is-home true

   cluster_B Aggregates:
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_B_1_aggr0 1.49TB  74.12GB 95% online       1 node_B_1
   raid4,

   mirror

   degraded
   ```

```
node_B_2_aggr0 1.49TB  74.12GB 95% online       1 node_B_2
raid4,

mirror

degraded
node_B_1_aggr1 2.99TB  2.88TB   3% online      15 node_B_1
raid_dp,

mirror

degraded
node_B_1_aggr2 2.99TB  2.91TB   3% online      14 node_B_1
raid_tec,

mirror

degraded
node_B_2_aggr1 2.95TB  2.80TB   5% online      37 node_B_2
raid_dp,

mirror

degraded
node_B_2_aggr2 2.99TB  2.87TB   4% online      35 node_B_2
raid_tec,

mirror

degraded
6 entries were displayed.

cluster_B::>
```

2. Identify the failed remote plexes:

   `storage aggregate plex show`

   The following example calls out the plexes that are remote (not plex0) and have a status of "failed":

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_1_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_1_aggr2 plex0 normal,active true     0
node_B_1_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr1 plex4 failed,inactive false  - <<<<---Plex at remote site
node_B_2_aggr2 plex0 normal,active true     0
node_B_2_aggr2 plex1 failed,inactive false  - <<<<---Plex at remote site
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
20 entries were displayed.

cluster_B::>
```

3. Take offline each of the failed plexes, and then delete them:

   a. Take offline the failed plexes:

      `storage aggregate plex offline -aggregate aggregate-name -plex plex-id`

      The following example shows the aggregate "node_B_2_aggr1/plex1" being taken offline:

      ```
      cluster_B::> storage aggregate plex offline -aggregate node_B_1_aggr0
      -plex plex4

      Plex offline successful on plex: node_B_1_aggr0/plex4
      ```

   b. Delete the failed plex:

      `storage aggregate plex delete -aggregate aggregate-name -plex plex-id`

      You can destroy the plex when prompted.

The following example shows the plex node_B_2_aggr1/plex1 being deleted.

```
cluster_B::> storage aggregate plex delete -aggregate  node_B_1_aggr0
-plex plex4

Warning: Aggregate "node_B_1_aggr0" is being used for the local
management root
         volume or HA partner management root volume, or has been
marked as
         the aggregate to be used for the management root volume
after a
         reboot operation. Deleting plex "plex4" for this aggregate
could lead
         to unavailability of the root volume after a disaster
recovery
         procedure. Use the "storage aggregate show -fields
         has-mroot,has-partner-mroot,root" command to view such
aggregates.

Warning: Deleting plex "plex4" of mirrored aggregate "node_B_1_aggr0"
on node
         "node_B_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you
want to
         destroy this plex? {y|n}: y
[Job 633] Job succeeded: DONE

cluster_B::>
```

You must repeat these steps for each of the failed plexes.

4. Confirm that the plexes have been removed:

```
storage aggregate plex show -fields aggregate,status,is-online,plex,pool
```

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

5. Identify the switched-over aggregates:

   `storage aggregate show -is-home false`

   You can also use the `storage aggregate plex show -fields aggregate,status,is-online,plex,pool` command to identify plex 0 switched-over aggregates. They will have a status of "failed, inactive".

   The following commands show four switched-over aggregates:

   - node_A_1_aggr1
   - node_A_1_aggr2
   - node_A_2_aggr1
   - node_A_2_aggr2

```
cluster_B::> storage aggregate show -is-home false

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.12TB  1.88TB   11% online      91 node_B_1
raid_dp,

mirror

degraded
node_A_1_aggr2 2.89TB  2.64TB    9% online      90 node_B_1
raid_tec,

mirror

degraded
node_A_2_aggr1 2.12TB  1.86TB   12% online      91 node_B_2
raid_dp,

mirror

degraded
node_A_2_aggr2 2.89TB  2.64TB    9% online      90 node_B_2
raid_tec,

mirror

degraded
4 entries were displayed.

cluster_B::>
```

6. Identify switched-over plexes:

   `storage aggregate plex show -fields aggregate,status,is-online,Plex,pool`

   You want to identify the plexes with a status of "failed, inactive".

   The following commands show four switched-over aggregates:

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_1_aggr2 plex0 normal,active true     0
node_B_2_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex0 failed,inactive false  -  <<<<-- Switched over
aggr/Plex0
node_A_2_aggr2 plex1 normal,active true     1
14 entries were displayed.

cluster_B::>
```

7. Delete the failed plex:

   ```
   storage aggregate plex delete -aggregate node_A_1_aggr1 -plex plex0
   ```

   You can destroy the plex when prompted.

   The following example shows the plex node_A_1_aggr1/plex0 being deleted:

```
cluster_B::> storage aggregate plex delete -aggregate node_A_1_aggr1
-plex plex0

Warning: Aggregate "node_A_1_aggr1" hosts MetroCluster metadata volume
         "MDV_CRS_e8457659b8a711e78b3b00a0988fe74b_A". Deleting plex
"plex0"
         for this aggregate can lead to the failure of configuration
         replication across the two DR sites. Use the "volume show
-vserver
         <admin-vserver> -volume MDV_CRS*" command to verify the
location of
         such volumes.

Warning: Deleting plex "plex0" of mirrored aggregate "node_A_1_aggr1" on
node
         "node_A_1" in a MetroCluster configuration will disable its
         synchronous disaster recovery protection. Are you sure you want
to
         destroy this plex? {y|n}: y
[Job 639] Job succeeded: DONE

cluster_B::>
```

You must repeat these steps for each of the failed aggregates.

8. Verify that there are no failed plexes remaining on the surviving site.

   The following output shows that all plexes are normal, active, and online.

```
cluster_B::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate    plex  status        is-online pool
------------ ----- ------------- --------- ----
node_B_1_aggr0 plex0 normal,active true     0
node_B_2_aggr0 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_B_1_aggr1 plex0 normal,active true     0
node_B_2_aggr2 plex0 normal,active true     0
node_A_1_aggr1 plex4 normal,active true     1
node_A_1_aggr2 plex1 normal,active true     1
node_A_2_aggr1 plex4 normal,active true     1
node_A_2_aggr2 plex1 normal,active true     1
10 entries were displayed.

cluster_B::>
```

Performing aggregate healing and restoring mirrors (MetroCluster IP configurations)

After replacing hardware and assigning disks, in systems running ONTAP 9.5 or earlier you can perform the MetroCluster healing operations. In all versions of ONTAP, you must then confirm that aggregates are mirrored and, if necessary, restart mirroring.

About this task

Starting with ONTAP 9.6, the healing operations are performed automatically when the disaster site nodes boot up. The healing commands are not required.

These steps are performed on the surviving cluster.

Steps

1. If you are using ONTAP 9.6 or later, you must verify that automatic healing completed successfully:
   a. Confirm that the heal-aggr-auto and heal-root-aggr-auto operations completed:

      ```
      metrocluster operation history show
      ```

      The following output shows that the operations have completed successfully on cluster_A.

```
cluster_B::*> metrocluster operation history show
Operation                     State          Start Time       End
Time
----------------------------- -------------- ----------------
----------------
heal-root-aggr-auto           successful      2/25/2019 06:45:58

2/25/2019 06:46:02
heal-aggr-auto                successful     2/25/2019 06:45:48

2/25/2019 06:45:52
.
.
.
```

b. Confirm that the disaster site is ready for switchback:

`metrocluster node show`

The following output shows that the operations have completed successfully on cluster_A.

```
cluster_B::*> metrocluster node show
DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1      configured     enabled   heal roots
completed
              node_A_2      configured     enabled   heal roots
completed
      cluster_B
              node_B_1      configured     enabled   waiting for
switchback recovery
              node_B_2      configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. If you are using ONTAP 9.5 or earlier, you must perform aggregate healing:

a. Verify the state of the nodes:

`metrocluster node show`

The following output shows that switchover has completed, so healing can be performed.

```
cluster_B::> metrocluster node show
DR                                  Configuration  DR
Group Cluster Node                  State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_B
              node_B_1           configured     enabled   switchover
completed
              node_B_2           configured     enabled   switchover
completed
      cluster_A
              node_A_1           configured     enabled   waiting for
switchback recovery
              node_A_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

b. Perform the aggregates healing phase:

`metrocluster heal -phase aggregates`

The following output shows a typical aggregates healing operation.

```
cluster_B::*> metrocluster heal -phase aggregates
[Job 647] Job succeeded: Heal Aggregates is successful.

cluster_B::*> metrocluster operation show
  Operation: heal-aggregates
      State: successful
 Start Time: 10/26/2017 12:01:15
   End Time: 10/26/2017 12:01:17
     Errors: -

cluster_B::*>
```

c. Verify that aggregate healing has completed and the disaster site is ready for switchback:

`metrocluster node show`

The following output shows that the "heal aggregates" phase has completed on cluster_A.

```
cluster_B::> metrocluster node show
DR                               Configuration  DR
Group Cluster Node               State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   heal
aggregates completed
              node_A_2           configured     enabled   heal
aggregates completed
      cluster_B
              node_B_1           configured     enabled   waiting for
switchback recovery
              node_B_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

3. If disks have been replaced, you must mirror the local and switched-over aggregates:
   a. Display the aggregates:

      `storage aggregate show`

```
cluster_B::> storage aggregate show
cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

normal
node_B_1_aggr1 3.14TB  3.04TB    3% online     15 node_B_1
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.06TB    3% online     14 node_B_1
raid_tec,
```

```
normal
node_B_1_aggr1 3.14TB  2.99TB    5% online     37 node_B_2
raid_dp,

normal
node_B_1_aggr2 3.14TB  3.02TB    4% online     35 node_B_2
raid_tec,

normal

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 2.36TB  2.12TB   10% online     91 node_B_1
raid_dp,

normal
node_A_1_aggr2 3.14TB  2.90TB    8% online     90 node_B_1
raid_tec,

normal
node_A_2_aggr1 2.36TB  2.10TB   11% online     91 node_B_2
raid_dp,

normal
node_A_2_aggr2 3.14TB  2.89TB    8% online     90 node_B_2
raid_tec,

normal
12 entries were displayed.

cluster_B::>
```

b. Mirror the aggregate:

`storage aggregate mirror -aggregate aggregate-name`

The following output shows a typical mirroring operation.

```
cluster_B::> storage aggregate mirror -aggregate node_B_1_aggr1

Info: Disks would be added to aggregate "node_B_1_aggr1" on node
"node_B_1" in
      the following manner:

      Second Plex

        RAID Group rg0, 6 disks (block checksum, raid_dp)
          Position   Disk                     Type
Size
          ---------- ------------------------ ----------
---------------
          dparity    5.20.6                   SSD
-
          parity     5.20.14                  SSD
-
          data       5.21.1                   SSD
894.0GB
          data       5.21.3                   SSD
894.0GB
          data       5.22.3                   SSD
894.0GB
          data       5.21.13                  SSD
894.0GB

      Aggregate capacity available for volume use would be 2.99TB.

Do you want to continue? {y|n}: y
```

c. Repeat the previous step for each of the aggregates from the surviving site.

d. Wait for the aggregates to resynchronize; you can check the status with the `storage aggregate show` command.

   The following output shows that a number of aggregates are resynchronizing.

```
cluster_B::> storage aggregate show

cluster_B Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_B_1_aggr0 1.49TB  74.12GB   95% online     1 node_B_1
raid4,
```

```
mirrored,

normal
node_B_2_aggr0 1.49TB  74.12GB   95% online     1 node_B_2
raid4,

mirrored,

normal
node_B_1_aggr1 2.86TB  2.76TB    4% online     15 node_B_1
raid_dp,

resyncing
node_B_1_aggr2 2.89TB  2.81TB    3% online     14 node_B_1
raid_tec,

resyncing
node_B_2_aggr1 2.73TB  2.58TB    6% online     37 node_B_2
raid_dp,

resyncing
node_B-2_aggr2 2.83TB  2.71TB    4% online     35 node_B_2
raid_tec,

resyncing

cluster_A Switched Over Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes
RAID Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1_aggr1 1.86TB  1.62TB   13% online     91 node_B_1
raid_dp,

resyncing
node_A_1_aggr2 2.58TB  2.33TB   10% online     90 node_B_1
raid_tec,

resyncing
node_A_2_aggr1 1.79TB  1.53TB   14% online     91 node_B_2
raid_dp,

resyncing
node_A_2_aggr2 2.64TB  2.39TB    9% online     90 node_B_2
raid_tec,
```

```
resyncing
12 entries were displayed.
```

e. Confirm that all aggregates are online and have resynchronized:

`storage aggregate plex show`

The following output shows that all aggregates have resynchronized.

```
cluster_A::> storage aggregate plex show
  ()
                    Is      Is          Resyncing
Aggregate Plex      Online  Resyncing    Percent Status
--------- --------- ------- ---------- --------- ---------------
node_B_1_aggr0 plex0 true    false              - normal,active
node_B_1_aggr0 plex8 true    false              - normal,active
node_B_2_aggr0 plex0 true    false              - normal,active
node_B_2_aggr0 plex8 true    false              - normal,active
node_B_1_aggr1 plex0 true    false              - normal,active
node_B_1_aggr1 plex9 true    false              - normal,active
node_B_1_aggr2 plex0 true    false              - normal,active
node_B_1_aggr2 plex5 true    false              - normal,active
node_B_2_aggr1 plex0 true    false              - normal,active
node_B_2_aggr1 plex9 true    false              - normal,active
node_B_2_aggr2 plex0 true    false              - normal,active
node_B_2_aggr2 plex5 true    false              - normal,active
node_A_1_aggr1 plex4 true    false              - normal,active
node_A_1_aggr1 plex8 true    false              - normal,active
node_A_1_aggr2 plex1 true    false              - normal,active
node_A_1_aggr2 plex5 true    false              - normal,active
node_A_2_aggr1 plex4 true    false              - normal,active
node_A_2_aggr1 plex8 true    false              - normal,active
node_A_2_aggr2 plex1 true    false              - normal,active
node_A_2_aggr2 plex5 true    false              - normal,active
20 entries were displayed.
```

4. On systems running ONTAP 9.5 and earlier, perform the root-aggregates healing phase:

`metrocluster heal -phase root-aggregates`

```
cluster_B::> metrocluster heal -phase root-aggregates
[Job 651] Job is queued: MetroCluster Heal Root Aggregates Job.Oct 26
13:05:00
[Job 651] Job succeeded: Heal Root Aggregates is successful.
```

5. Verify that the "heal roots" phase has completed and the disaster site is ready for switchback:

   The following output shows that the "heal roots" phase has completed on cluster_A.

```
cluster_B::> metrocluster node show
DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1           configured     enabled   heal roots
completed
              node_A_2           configured     enabled   heal roots
completed
      cluster_B
              node_B_1           configured     enabled   waiting for
switchback recovery
              node_B_2           configured     enabled   waiting for
switchback recovery
4 entries were displayed.

cluster_B::>
```

Proceed to verify the licenses on the replaced nodes.

Verifying licenses on the replaced nodes

Preparing for switchback in a MetroCluster FC configuration

You must perform certain tasks in order to prepare the MetroCluster FC configuration for the switchback operation.

Verifying port configuration (MetroCluster FC configurations only)

You must set the environmental variables on the node and then power it off to prepare it for MetroCluster configuration.

About this task

This procedure is performed with the replacement controller modules in Maintenance mode.

The steps to check configuration of ports is needed only on systems in which FC or CNA ports are used in initiator mode.

Steps

1. In Maintenance mode, enter the following command to restore the FC port configuration:

   `ucadmin modify -m fc -t initiatoradapter_name`

   If you only want to use one of a port pair in the initiator configuration, enter a precise adapter name.

2. Take one of the following actions, depending on your configuration:

If the FC port configuration is…	Then…
The same for both ports	Answer `y` when prompted by the system, because modifying one port in a port pair also modifies the other port.
Different	a. Answer `n` when prompted by the system. b. Enter the following command to restore the FC port configuration: `ucadmin modify -m fc -t initiator|targetadapter_name`

3. Exit Maintenance mode by entering the following command: `halt`

   After you issue the command, wait until the system stops at the LOADER prompt.

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

   `boot_ontap maint`

5. Verify the values of the variables by entering the following command:

   `ucadmin show`

6. Exit Maintenance mode and display the LOADER prompt: `halt`

Configuring the FC-to-SAS bridges (MetroCluster FC configurations only)

If you replaced the FC-to-SAS bridges, you must configure them when restoring the MetroCluster configuration. The procedure is identical to the initial configuration of an FC-to-SAS bridge.

Steps

1. Power on the FC-to-SAS bridges.
2. Set the IP address on the Ethernet ports by using the `set IPAddress port ipaddress` command.
   - `port` can be either "MP1" or "MP2".
   - `ipaddress` can be an IP address in the format xxx.xxx.xxx.xxx.

In the following example, the IP address is 10.10.10.55 on Ethernet port 1:

```
Ready.
set IPAddress MP1 10.10.10.55

Ready. *
```

3. Set the IP subnet mask on the Ethernet ports by using the `set IPSubnetMask port mask` command.
   - `port` can be "MP1" or "MP2".
   - `mask` can be a subnet mask in the format xxx.xxx.xxx.xxx.

   In the following example, the IP subnet mask is 255.255.255.0 on Ethernet port 1:

```
Ready.
set IPSubnetMask MP1 255.255.255.0

Ready. *
```

4. Set the speed on the Ethernet ports by using the `set EthernetSpeed port speed` command.
   - `port` can be "MP1" or "MP2".
   - `speed` can be "100", "1000", or "auto".

   In the following example, the Ethernet speed is set to 1000 on Ethernet port 1.

```
Ready.
set EthernetSpeed MP1 1000

Ready. *
```

5. Save the configuration by using the `saveConfiguration` command, and restart the bridge when prompted to do so.

   Saving the configuration after configuring the Ethernet ports enables you to proceed with the bridge configuration using Telnet and enables you to access the bridge using FTP to perform firmware updates.

   The following example shows the `saveConfiguration` command and the prompt to restart the bridge.

```
Ready.
SaveConfiguration
  Restart is necessary....
  Do you wish to restart (y/n) ?
Confirm with 'y'. The bridge will save and restart with the new
settings.
```

6. After the FC-to-SAS bridge reboots, log in again.
7. Set the speed on the FC ports by using the `set fcdatarate port speed` command.
   - `port` can be "1" or "2".
   - `speed` can be "2 Gb", "4 Gb", "8 Gb", or "16 Gb", depending on your model bridge.

   In the following example, the port FC1 speed is set to "8 Gb".

   ```
   Ready.
   set fcdatarate 1 8Gb

   Ready. *
   ```

8. Set the topology on the FC ports by using the `set FCConnMode port mode` command.
   - `port` can be "1" or "2".
   - `mode` can be "ptp", "loop", "ptp-loop", or "auto".

   In the following example, the port FC1 topology is set to "ptp".

   ```
   Ready.
   set FCConnMode 1 ptp

   Ready. *
   ```

9. Save the configuration by using the `saveConfiguration` command, and restart the bridge when prompted to do so.

   The following example shows the `saveConfiguration` command and the prompt to restart the bridge.

```
 Ready.
 SaveConfiguration
    Restart is necessary....
    Do you wish to restart (y/n) ?
 Confirm with 'y'. The bridge will save and restart with the new
settings.
```

10. After the FC-to-SAS bridge reboots, log in again.
11. If the FC-to-SAS bridge is running firmware 1.60 or later, enable SNMP.

```
Ready.
set snmp enabled

Ready. *
saveconfiguration

Restart is necessary....
Do you wish to restart (y/n) ?

Verify with 'y' to restart the FibreBridge.
```

12. Power off the FC-to-SAS bridges.

Configuring the FC switches (MetroCluster FC configurations only)

If you have replaced the FC switches in the disaster site, you must configure them using the vendor-specific procedures. You must configure one switch, verify that storage access on the surviving site is not impacted, and then configure the second switch.

Related tasks

Port assignments for FC switches when using 9.0

Port assignments for FC switches when using ONTAP 9.1 and later

Configuring a Brocade FC switch after site disaster

You must use this Brocade-specific procedure to configure the replacement switch and enable the ISL ports.

About this task

The examples in this procedure are based on the following assumptions:

- Site A is the disaster site.
- FC_switch_A_1 has been replaced.
- FC_switch_A_2 has been replaced.
- Site B is the surviving site.
- FC_switch_B_1 is healthy.
- FC_switch_B_2 is healthy.

You must verify that you are using the specified port assignments when you cable the FC switches:

- Port assignments for FC switches when using ONTAP 9.0
- Port assignments for FC switches when using ONTAP 9.1 and later

The examples show two FC-to-SAS bridges. If you have more bridges, you must disable and subsequently enable the additional ports.

Steps

1. Boot and pre-configure the new switch:
    a. Power up the new switch and let it boot up.
    b. Check the firmware version on the switch to confirm it matches the version of the other FC switches:

        `firmwareShow`

    c. Configure the new switch as described in the following topics, skipping the steps for configuring zoning on the switch.

        Fabric-attached MetroCluster installation and configuration

        Stretch MetroCluster installation and configuration

    d. Disable the switch persistently:

        `switchcfgpersistentdisable`

        The switch will remain disabled after a reboot or fastboot. If this command is not available, you should use the `switchdisable` command.

        The following example shows the command on BrocadeSwitchA:

```
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

        The following example shows the command on BrocadeSwitchB:

```
BrocadeSwitchA:admin> switchcfgpersistentdisable
```

2. Complete configuration of the new switch:
    a. Enable the ISLs on the surviving site:

        `portcfgpersistentenable port-number`

```
FC_switch_B_1:admin> portcfgpersistentenable 10
FC_switch_B_1:admin> portcfgpersistentenable 11
```

    b. Enable the ISLs on the replacement switches:

        `portcfgpersistentenable port-number`

```
FC_switch_A_1:admin> portcfgpersistentenable 10
FC_switch_A_1:admin> portcfgpersistentenable 11
```

c. On the replacement switch (FC_switch_A_1 in this example) verify that the ISL's are online:

`switchshow`

```
FC_switch_A_1:admin> switchshow
switchName: FC_switch_A_1
switchType: 71.2
switchState:Online
switchMode: Native
switchRole: Principal
switchDomain:       4
switchId:   fffc03
switchWwn:  10:00:00:05:33:8c:2e:9a
zoning:             OFF
switchBeacon:       OFF

Index Port Address Media Speed State  Proto
==============================================
...
10   10    030A00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1"
11   11    030B00 id   16G     Online  FC E-Port
10:00:00:05:33:86:89:cb "FC_switch_A_1" (downstream)
...
```

3. Persistently enable the switch:

   `switchcfgpersistentenable`

4. Verify that the ports are online:

   `switchshow`

Configuring a Cisco FC switch after site disaster

You must use the Cisco-specific procedure to configure the replacement switch and enable the ISL ports.

About this task

The examples in this procedure are based on the following assumptions:

- Site A is the disaster site.

- FC_switch_A_1 has been replaced.
- FC_switch_A_2 has been replaced.
- Site B is the surviving site.
- FC_switch_B_1 is healthy.
- FC_switch_B_2 is healthy.

Steps

1. Configure the switch:
   a. Refer to Fabric-attached MetroCluster installation and configuration
   b. Follow the steps for configuring the switch in Configuring the Cisco FC switches section, *except* for the "Configuring zoning on a Cisco FC switch" section:

      Zoning is configured later in this procedure.

2. On the healthy switch (in this example, FC_switch_B_1), enable the ISL ports.

   The following example shows the commands to enable the ports:

```
FC_switch_B_1# conf t
FC_switch_B_1(config)# int fc1/14-15
FC_switch_B_1(config)# no shut
FC_switch_B_1(config)# end
FC_switch_B_1# copy running-config startup-config
FC_switch_B_1#
```

3. Verify that the ISL ports are up by using the show interface brief command.
4. Retrieve the zoning information from the fabric.

   The following example shows the commands to distribute the zoning configuration:

```
FC_switch_B_1(config-zone)# zoneset distribute full vsan 10
FC_switch_B_1(config-zone)# zoneset distribute full vsan 20
FC_switch_B_1(config-zone)# end
```

   FC_switch_B_1 is distributed to all other switches in the fabric for "vsan 10" and "vsan 20", and the zoning information is retrieved from FC_switch_A_1.

5. On the healthy switch, verify that the zoning information is properly retrieved from the partner switch:

   `show zone`

```
FC_switch_B_1# show zone
zone name FC-VI_Zone_1_10 vsan 10
  interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25A vsan 20
  interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

zone name STOR_Zone_1_20_25B vsan 20
  interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
  interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
  interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

6. Determine the worldwide names (WWNs) of the switches in the switch fabric.

   In this example, the two switch WWNs are as follows:

   - FC_switch_A_1: 20:00:54:7f:ee:b8:24:c0
   - FC_switch_B_1: 20:00:54:7f:ee:c6:80:78

```
FC_switch_B_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:c6:80:78
FC_switch_B_1#

FC_switch_A_1# show wwn switch
Switch WWN is 20:00:54:7f:ee:b8:24:c0
FC_switch_A_1#
```

7. Enter configuration mode for the zone and remove zone members that do not belong to the switch WWNs of the two switches:

```
no member interface interface-ide swwn wwn
```

In this example, the following members are not associated with the WWN of either of the switches in the fabric and must be removed:

   - Zone name FC-VI_Zone_1_10 vsan 10
      - Interface fc1/1 swwn 20:00:54:7f:ee:e3:86:50
      - Interface fc1/2 swwn 20:00:54:7f:ee:e3:86:50

   > AFF A700 and FAS9000 systems support four FC-VI ports. You must remove all four ports from the FC-VI zone.

   - Zone name STOR_Zone_1_20_25A vsan 20
      - Interface fc1/5 swwn 20:00:54:7f:ee:e3:86:50
      - Interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
      - Interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
      - Interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
      - Interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50
   - Zone name STOR_Zone_1_20_25B vsan 20
      - Interface fc1/8 swwn 20:00:54:7f:ee:e3:86:50
      - Interface fc1/9 swwn 20:00:54:7f:ee:e3:86:50
      - Interface fc1/10 swwn 20:00:54:7f:ee:e3:86:50
      - Interface fc1/11 swwn 20:00:54:7f:ee:e3:86:50

The following example shows the removal of these interfaces:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# no member interface fc1/1 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/2 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/5 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# no member interface fc1/8 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/9 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/10 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# no member interface fc1/11 swwn
20:00:54:7f:ee:e3:86:50
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

8. Add the ports of the new switch to the zones.

   The following example assumes that the cabling on the replacement switch is the same as on the old switch:

```
 FC_switch_B_1# conf t
 FC_switch_B_1(config)# zone name FC-VI_Zone_1_10 vsan 10
 FC_switch_B_1(config-zone)# member interface fc1/1 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/2 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25A vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/5 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# zone name STOR_Zone_1_20_25B vsan 20
 FC_switch_B_1(config-zone)# member interface fc1/8 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/9 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/10 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# member interface fc1/11 swwn
20:00:54:7f:ee:c6:80:78
 FC_switch_B_1(config-zone)# save running-config startup-config
 FC_switch_B_1(config-zone)# zoneset distribute full 10
 FC_switch_B_1(config-zone)# zoneset distribute full 20
 FC_switch_B_1(config-zone)# end
 FC_switch_B_1# copy running-config startup-config
```

9. Verify that the zoning is properly configured: `show zone`

   The following example output shows the three zones:

```
FC_switch_B_1# show zone
  zone name FC-VI_Zone_1_10 vsan 10
    interface fc1/1 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/2 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/1 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/2 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25A vsan 20
    interface fc1/5 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0

  zone name STOR_Zone_1_20_25B vsan 20
    interface fc1/8 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/9 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/10 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/11 swwn 20:00:54:7f:ee:c6:80:78
    interface fc1/5 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/8 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/9 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/10 swwn 20:00:54:7f:ee:b8:24:c0
    interface fc1/11 swwn 20:00:54:7f:ee:b8:24:c0
FC_switch_B_1#
```

Verifying the storage configuration

You must confirm that all storage is visible from the surviving nodes.

Steps

1. Confirm that all storage components at the disaster site are the same in quantity and type at the surviving site.

   The surviving site and disaster site should have the same number of disk shelf stacks, disk shelves, and disks. In a bridge-attached or fabric-attached MetroCluster configuration, the sites should have the same number of FC-to-SAS bridges.

2. Confirm that all disks that have been replaced at the disaster site are unowned:

   `run local disk show-n`

   Disks should appear as being unowned.

3. If no disks were replaced, confirm that all disks are present:

   `disk show`

Powering on the equipment at the disaster site

You must power on the MetroCluster components at the disaster site when you are ready to prepare for switchback. In addition, you must also recable the SAS storage connections in direct-attached MetroCluster configurations and enable non-Inter-Switch Link ports in fabric-attached MetroCluster configurations.

Before you begin

You must have already replaced and cabled the MetroCluster components exactly as the old ones.

[Fabric-attached MetroCluster installation and configuration](#)

[Stretch MetroCluster installation and configuration](#)

About this task

The examples in this procedure assume the following:

- Site A is the disaster site.
  - FC_switch_A_1 has been replaced.
  - FC_switch_A_2 has been replaced.
- Site B is the surviving site.
  - FC_switch_B_1 is healthy.
  - FC_switch_B_2 is healthy.

The FC switches are present only in fabric-attached MetroCluster configurations.

Steps

1. In a stretch MetroCluster configuration using SAS cabling (and no FC switch fabric or FC-to-SAS bridges), connect all the storage including the remote storage across both sites.

   The controller at the disaster site must remain powered off or at the LOADER prompt.

2. On the surviving site, disable disk autoassignment:

   `storage disk option modify -autoassign off *`

   ```
   cluster_B::> storage disk option modify -autoassign off *
   2 entries were modified.
   ```

3. On the surviving site, confirm that disk autoassignment is off:

   `storage disk option show`

```
cluster_B::> storage disk option show
Node      BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on            on          off              default
node_B_2       on            on          off              default
2 entries were displayed.

 cluster_B::>
```

4. Turn on the disk shelves at the disaster site and make sure that all disks are running.
5. In a bridge-attached or fabric-attached MetroCluster configuration, turn on all FC-to-SAS bridges at the disaster site.
6. If any disks were replaced, leave the controllers powered off or at the LOADER prompt.
7. In a fabric-attached MetroCluster configuration, enable the non-ISL ports on the FC switches.

If the switch vendor is…	Then use these steps to enable the ports…

<table>
<tr>
<td>Brocade</td>
<td>

a. Persistently enable the ports connected to the FC-to-SAS bridges: `portpersistentenable port-number`

In the following example, ports 6 and 7 are enabled:

```
FC_switch_A_1:admin>
portpersistentenable 6
FC_switch_A_1:admin>
portpersistentenable 7

FC_switch_A_1:admin>
```

b. Persistently enable the ports connected to the HBAs and FC-VI adapters: `portpersistentenable port-number`

In the following example, ports 6 and 7 are enabled:

```
FC_switch_A_1:admin>
portpersistentenable 1
FC_switch_A_1:admin>
portpersistentenable 2
FC_switch_A_1:admin>
portpersistentenable 4
FC_switch_A_1:admin>
portpersistentenable 5
FC_switch_A_1:admin>
```

For AFF A700 and FAS9000 systems, you must persistently enable all four FC-VI ports by using the switchcfgpersistentenable command.

c. Repeat substeps a and b for the second FC switch at the surviving site.

</td>
</tr>
</table>

Cisco	a. Enter configuration mode for the interface, and then enable the ports with the no shut command.
	
	In the following example, port fc1/36 is disabled:
	
	`FC_switch_A_1# conf t`
	`FC_switch_A_1(config)# interface fc1/36`
	`FC_switch_A_1(config)# no shut`
	`FC_switch_A_1(config-if)# end`
	`FC_switch_A_1# copy running-config startup-config`
	
	b. Verify that the switch port is enabled: `show interface brief`
	
	c. Repeat Substeps a and b on the other ports connected to the FC-to-SAS bridges, HBAs, and FC-VI adapters.
	
	d. Repeat Substeps a, b, and c for the second FC switch at the surviving site.

Assigning ownership for replaced drives

If you replaced drives when restoring hardware at the disaster site or you had to zero drives or remove ownership, you must assign ownership to the affected drives.

Before you begin

The disaster site must have at least as many available drives as it did prior to the disaster.

The drives shelves and drives arrangement must meet the requirements in Required MetroCluster IP component and naming conventions section of the MetroCluster IP Installation and Configuration Guide.

About this task

These steps are performed on the cluster at the disaster site.

This procedure shows the reassignment of all drives and the creation of new plexes at the disaster site. The new plexes are remote plexes of surviving site and local plexes of disaster site.

This section provides examples for two and four-node configurations. For two-node configurations, you can ignore references to the second node at each site. For eight-node configurations, you must account for the additional nodes on the second DR group. The examples make the following assumptions:

- Site A is the disaster site.
  - node_A_1 has been replaced.
  - node_A_2 has been replaced.

Present only in four-node MetroCluster configurations.

- Site B is the surviving site.
  - node_B_1 is healthy.
  - node_B_2 is healthy.

    Present only in four-node MetroCluster configurations.

The controller modules have the following original system IDs:

Number of nodes in MetroCluster configuration	Node	Original system ID
Four	node_A_1	4068741258
node_A_2	4068741260	node_B_1
4068741254	node_B_2	4068741256
Two	node_A_1	4068741258

You should keep in mind the following points when assigning the drives:

- The old-count-of-disks must be at least the same number of disks for each node that were present before the disaster.

  If a lower number of disks is specified or present, the healing operations might not be completed due to insufficient space.

- The new plexes to be created are remote plexes belonging to the surviving site (node_B_x pool1) and local plexes belonging to the disaster site (node_B_x pool0).
- The total number of required drives should not include the root aggr disks.

  If n disks are assigned to pool1 of the surviving site, then n-3 disks should be assigned to the disaster site with the assumption that the root aggregate uses three disks.

- None of the disks can be assigned to a pool that is different from the one to which all other disks on the same stack are assigned.
- Disks belonging to the surviving site are assigned to pool 1 and disks belonging to the disaster site are assigned to pool 0.

Steps

1. Assign the new, unowned drives based on whether you have a four-node or two-node MetroCluster configuration:
   - For four-node MetroCluster configurations, assign the new, unowned disks to the appropriate disk pools by using the following series of commands on the replacement nodes:
     i. Systematically assign the replaced disks for each node to their respective disk pools:

        ```
        disk assign -s sysid -n old-count-of-disks -p pool
        ```

From the surviving site, you issue a disk assign command for each node:

```
cluster_B::> disk assign -s node_B_1-sysid -n old-count-of-disks
-p 1 **\(remote pool of surviving site\)**
cluster_B::> disk assign -s node_B_2-sysid -n old-count-of-disks
-p 1 **\(remote pool of surviving site\)**
cluster_B::> disk assign -s node_A_1-old-sysid -n old-count-of-
disks -p 0 **\(local pool of disaster site\)**
cluster_B::> disk assign -s node_A_2-old-sysid -n old-count-of-
disks -p 0 **\(local pool of disaster site\)**
```

The following example shows the commands with the system IDs:

```
cluster_B::> disk assign -s 4068741254 -n 21 -p 1
cluster_B::> disk assign -s 4068741256 -n 21 -p 1
cluster_B::> disk assign -s 4068741258 -n 21 -p 0
cluster_B::> disk assign -s 4068741260 -n 21 -p 0
```

ii. Confirm the ownership of the disks:

```
storage disk show -fields owner, pool
```

```
storage disk show -fields owner, pool
cluster_A::> storage disk show -fields owner, pool
disk     owner          pool
-------- ------------- -----
0c.00.1  node_A_1      Pool0
0c.00.2  node_A_1      Pool0
.
.
.
0c.00.8  node_A_1      Pool1
0c.00.9  node_A_1      Pool1
.
.
.
0c.00.15 node_A_2      Pool0
0c.00.16 node_A_2      Pool0
.
.
.
0c.00.22 node_A_2      Pool1
0c.00.23 node_A_2      Pool1
.
.
.
```

- For two-node MetroCluster configurations, assign the new, unowned disks to the appropriate disk pools by using the following series of commands on the replacement node:

  i. Display the local shelf IDs:

  ```
  run local storage show shelf
  ```

  ii. Assign the replaced disks for the healthy node to pool 1:

  ```
  run local disk assign -shelf shelf-id -n old-count-of-disks -p 1 -s
  node_B_1-sysid -f
  ```

  iii. Assign the replaced disks for the replacement node to pool 0:

  ```
  run local disk assign -shelf shelf-id -n old-count-of-disks -p 0 -s
  node_A_1-sysid -f
  ```

2. On the surviving site, turn on automatic disk assignment again:

```
storage disk option modify -autoassign on *
```

```
cluster_B::> storage disk option modify -autoassign on *
2 entries were modified.
```

3. On the surviving site, confirm that automatic disk assignment is on:

   `storage disk option show`

```
 cluster_B::> storage disk option show
 Node     BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
--------  -------------  -----------  -----------  ------------------
node_B_1       on             on          on              default
node_B_2       on             on          on              default
2 entries were displayed.

 cluster_B::>
```

Related information

Disk and aggregate management

How MetroCluster configurations use SyncMirror to provide data redundancy

Performing aggregate healing and restoring mirrors (MetroCluster FC configurations)

After replacing hardware and assigning disks, you can perform the MetroCluster healing operations. You must then confirm that aggregates are mirrored and, if necessary, restart mirroring.

Steps

1. Perform the two phases of healing (aggregate healing and root healing) on the disaster site:

```
cluster_B::> metrocluster heal -phase aggregates

cluster_B::> metrocluster heal -phase root aggregates
```

2. Monitor the healing and verify that the aggregates are in either the resyncing or mirrored state:

   `storage aggregate show -node local`

If the aggregate shows this state…	Then…
resyncing	No action is required. Let the aggregate complete resyncing.
mirror degraded	Proceed to Step 3

mirrored, normal	No action is required.
unknown, offline	The root aggregate shows this state if all the disks on the disaster sites were replaced.

```
cluster_B::> storage aggregate show -node local

 Aggregate     Size Available Used% State   #Vols  Nodes      RAID
Status
 --------- -------- --------- ----- ------- ------ ----------
------------
 node_B_1_aggr1
            227.1GB   11.00GB   95% online       1 node_B_1   raid_dp,
                                                              resyncing
 NodeA_1_aggr2
            430.3GB   28.02GB   93% online       2 node_B_1   raid_dp,
                                                              mirror
                                                              degraded
 node_B_1_aggr3
            812.8GB   85.37GB   89% online       5 node_B_1   raid_dp,
                                                              mirrored,
                                                              normal
 3 entries were displayed.

cluster_B::>
```

In the following examples, the three aggregates are each in a different state:

Node	State
node_B_1_aggr1	resyncing
node_B_1_aggr2	mirror degraded
node_B_1_aggr3	mirrored, normal

3. If one or more plexes remain offline, additional steps are required to rebuild the mirror.

In the preceding table, the mirror for node_B_1_aggr2 must be rebuilt.

a. View details of the aggregate to identify any failed plexes:

```
storage aggregate show -r -aggregate node_B_1_aggr2
```

In the following example, plex /node_B_1_aggr2/plex0 is in a failed state:

```
cluster_B::> storage aggregate show -r -aggregate node_B_1_aggr2

 Owner Node: node_B_1
  Aggregate: node_B_1_aggr2 (online, raid_dp, mirror degraded) (block
checksums)
   Plex: /node_B_1_aggr2/plex0 (offline, failed, inactive, pool0)
    RAID Group /node_B_1_aggr2/plex0/rg0 (partial)
                                                              Usable
Physical
      Position Disk                     Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------

   Plex: /node_B_1_aggr2/plex1 (online, normal, active, pool1)
    RAID Group /node_B_1_aggr2/plex1/rg0 (normal, block checksums)
                                                              Usable
Physical
      Position Disk                     Pool Type     RPM     Size
Size Status
      -------- ------------------------ ---- ----- ------ --------
-------- ----------
      dparity  1.44.8                    1   SAS    15000  265.6GB
273.5GB (normal)
      parity   1.41.11                   1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.42.8                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.11                   1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.44.9                    1   SAS    15000  265.6GB
273.5GB (normal)
      data     1.43.18                   1   SAS    15000  265.6GB
273.5GB (normal)
 6 entries were displayed.

 cluster_B::>
```

b. Delete the failed plex:

```
storage aggregate plex delete -aggregate aggregate-name -plex plex
```

c. Reestablish the mirror:

```
storage aggregate mirror -aggregate aggregate-name
```

d. Monitor the resynchronization and mirroring status of the plex until all mirrors are reestablished and all aggregates show mirrored, normal status:

```
storage aggregate show
```

Reassigning disk ownership for root aggregates to replacement controller modules (MetroCluster FC configurations)

If one or both of the controller modules or NVRAM cards were replaced at the disaster site, the system ID has changed and you must reassign disks belonging to the root aggregates to the replacement controller modules.

About this task

Because the nodes are in switchover mode and healing has been done, only the disks containing the root aggregates of pool1 of the disaster site will be reassigned in this section. They are the only disks still owned by the old system ID at this point.

This section provides examples for two and four-node configurations. For two-node configurations, you can ignore references to the second node at each site. For eight-node configurations, you must account for the additional nodes on the second DR group. The examples make the following assumptions:

- Site A is the disaster site.
  - node_A_1 has been replaced.
  - node_A_2 has been replaced.

    Present only in four-node MetroCluster configurations.
- Site B is the surviving site.
  - node_B_1 is healthy.
  - node_B_2 is healthy.

    Present only in four-node MetroCluster configurations.

The old and new system IDs were identified in Determining the system IDs of the replacement controller modules.

The examples in this procedure use controllers with the following system IDs:

Number of nodes	Node	Original system ID	New system ID
Four	node_A_1	4068741258	1574774970
	node_A_2	4068741260	1574774991
	node_B_1	4068741254	unchanged
	node_B_2	4068741256	unchanged
Two	node_A_1	4068741258	1574774970

Steps

1. With the replacement node in Maintenance mode, reassign the root aggregate disks:

   `disk reassign -s old-system-ID -d new-system-ID`

   ```
   *> disk reassign -s 4068741258 -d 1574774970
   ```

2. View the disks to confirm the ownership change of the pool1 root aggr disks of the disaster site to the replacement node:

   `disk show`

   The output might show more or fewer disks, depending on how many disks are in the root aggregate and whether any of these disks failed and were replaced. If the disks were replaced, then Pool0 disks will not appear in the output.

   The pool1 root aggregate disks of the disaster site should now be assigned to the replacement node.

   ```
   *> disk show
   Local System ID: 1574774970

     DISK              OWNER                POOL   SERIAL NUMBER   HOME
   DR HOME
   ------------       -------------        -----  -------------
   -------------       -------------
   sw_A_1:6.126L19    node_A_1(1574774970) Pool0  serial-number
   node_A_1(1574774970)
   sw_A_1:6.126L3     node_A_1(1574774970) Pool0  serial-number
   node_A_1(1574774970)
   sw_A_1:6.126L7     node_A_1(1574774970) Pool0  serial-number
   node_A_1(1574774970)
   sw_B_1:6.126L8     node_A_1(1574774970) Pool1  serial-number
   node_A_1(1574774970)
   sw_B_1:6.126L24    node_A_1(1574774970) Pool1  serial-number
   node_A_1(1574774970)
   sw_B_1:6.126L2     node_A_1(1574774970) Pool1  serial-number
   node_A_1(1574774970)

   *> aggr status
            Aggr State           Status
    node_A_1_root online          raid_dp, aggr
                                  mirror degraded
                                  64-bit
   *>
   ```

3. View the aggregate status:

```
aggr status
```

The output might show more or fewer disks, depending on how many disks are in the root aggregate and whether any of these disks failed and were replaced. If disks were replaced, then Pool0 disks will not appear in output.

```
*> aggr status
           Aggr State           Status
  node_A_1_root online           raid_dp, aggr
                                 mirror degraded
                                 64-bit
*>
```

4. Delete the contents of the mailbox disks:

   ```
   mailbox destroy local
   ```

5. If the aggregate is not online, bring it online:

   ```
   aggr online aggr_name
   ```

6. Halt the node to display the LOADER prompt:

   ```
   halt
   ```

Booting the new controller modules (MetroCluster FC configurations)

After aggregate healing has been completed for both the data and root aggregates, you must boot the node or nodes at the disaster site.

About this task

This task begins with the nodes showing the LOADER prompt.

Steps

1. Display the boot menu:

   ```
   boot_ontap menu
   ```

2. From the boot menu, select option 6, **Update flash from backup config**.
3. Respond `y` to the following prompt:

   ```
   This will replace all flash-based configuration with the last backup to disks.
   Are you sure you want to continue?: y
   ```

   The system will boot twice, the second time to load the new configuration.

> If you did not clear the NVRAM contents of a used replacement controller, then you might see a panic with the following message: `PANIC: NVRAM contents are invalid...` If this occurs, repeat Step 2 to boot the system to the ONTAP prompt. You will then need to perform a root recovery. Contact technical support for assistance.

4. Mirror the root aggregate on plex 0:
   a. Assign three pool0 disks to the new controller module.
   b. Mirror the root aggregate pool1 plex:

      ```
      aggr mirror root-aggr-name
      ```

   c. Assign unowned disks to pool0 on the local node
5. Refresh the MetroCluster configuration:
   a. Enter advanced privilege mode:

      ```
      set -privilege advanced
      ```

   b. Refresh the configuration:

      ```
      metrocluster configure -refresh true
      ```

   c. Return to admin privilege mode:

      ```
      set -privilege admin
      ```

6. If you have a four-node configuration, repeat the previous steps on the other node at the disaster site.

Proceed to Complete the disaster recovery process.

Preparing for switchback in a mixed configuration (recovery during transition)

You must perform certain tasks in order to prepare the mixed MetroCluster IP and FC configuration for the switchback operation. This procedure only applies to configurations that encountered a failure during the MetroCluster FC to IP transition process.

About this task

This procedure should only be used when performing recovery on a system that was in mid-transition when the failure occurred.

In this scenario, the MetroCluster is a mixed configuration:

- One DR group consists of fabric-attached MetroCluster FC nodes.

  You must perform the MetroCluster FC recovery steps on these nodes.

- One DR group consists of MetroCluster IP nodes.

  You must perform the MetroCluster IP recovery steps on these nodes.

Steps

Perform the steps in the following order.

1. Prepare the FC nodes for switchback by performing the following tasks in order:
   a. Verifying port configuration (MetroCluster FC configurations only)
   b. Configuring the FC-to-SAS bridges (MetroCluster FC configurations only)
   c. Configuring the FC switches (MetroCluster FC configurations only)
   d. Verifying the storage configuration (only perform these steps on replaced drives on the MetroCluster FC nodes)
   e. Powering on the equipment at the disaster site (only perform these steps on replaced drives on the MetroCluster FC nodes)
   f. Assigning ownership for replaced drives (only perform these steps on replaced drives on the MetroCluster FC nodes)
   g. Perform the steps in Reassigning disk ownership for root aggregates to replacement controller modules (MetroCluster FC configurations), up to and including the step to issue the mailbox destroy command.
   h. Destroy the local plex (plex 0) of the root aggregate:

      ```
      aggr destroy plex-id
      ```

   i. If the root aggr is not online, bring it online.
2. Boot the MetroCluster FC nodes.

   You must perform these steps on both of the MetroCluster FC nodes.

   a. Display the boot menu:

      ```
      boot_ontap menu
      ```

   b. From the boot menu, select option 6, **Update flash from backup config**.
   c. Respond `y` to the following prompt:

      ```
      This will replace all flash-based configuration with the last backup to
      disks. Are you sure you want to continue?: y
      ```

      The system will boot twice, the second time to load the new configuration.

      > If you did not clear the NVRAM contents of a used replacement controller, then you might see a panic with the following message: `PANIC: NVRAM contents are invalid...` If this occurs, repeat these substeps to boot the system to the ONTAP prompt. You will then need to perform a root recovery. Contact technical support for assistance.

3. Mirror the root aggregate on plex 0:

   You must perform these steps on both of the MetroCluster FC nodes.

   a. Assign three pool0 disks to the new controller module.
   b. Mirror the root aggregate pool1 plex:

      ```
      aggr mirror root-aggr-name
      ```

c. Assign unowned disks to pool0 on the local node

4. Return to Maintenance mode.

   You must perform these steps on both of the MetroCluster FC nodes.

   a. Halt the node:

      `halt`

   b. Boot the node to Maintenance:

      `mode:boot_ontap maint`

5. Delete the contents of the mailbox disks:

   `mailbox destroy local`

   You must perform these steps on both of the MetroCluster FC nodes.

6. Halt the nodes:
   `halt`

7. After the nodes boot up, verify the status of the node:

   `metrocluster node show`

```
siteA::*> metrocluster node show
DR                                Configuration  DR
Group Cluster Node                State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     siteA
              wmc66-a1           configured     enabled   waiting for
switchback recovery
              wmc66-a2           configured     enabled   waiting for
switchback recovery
      siteB
              wmc66-b1           configured     enabled   switchover
completed
              wmc66-b2           configured     enabled   switchover
completed
2     siteA
              wmc55-a1           -              -         -
              wmc55-a2           unreachable    -         -
      siteB
              wmc55-b1           configured     enabled   switchover
completed
              wmc55-b2           configured
```

8. Prepare the MetroCluster IP nodes for switchback by performing the tasks in Preparing for switchback in a MetroCluster IP configuration up to and including Deleting failed plexes owned by the surviving site (MetroCluster IP configurations).
9. On the MetroCluster FC nodes, perform the steps in Performing aggregate healing and restoring mirrors (MetroCluster FC configurations).
10. On the MetroCluster IP nodes, perform the steps in Performing aggregate healing and restoring mirrors (MetroCluster IP configurations).
11. Proceed through the remaining tasks of the recovery process starting with Reestablishing object stores for FabricPool configurations.

Completing recovery

Reestablishing object stores for FabricPool configurations

If one of the object stores in a FabricPool mirror was co-located with the MetroCluster disaster site and was destroyed, you must reestablish the object store and the FabricPool mirror.

About this task

- If the object-stores are remote and a MetroCluster site is destroyed, you do not need to rebuild the object store, and the original object store configurations as well as cold data contents are retained.
- For more information about FabricPool configurations, see the Disk and Aggregates Power Guide.

Step

1. Follow the procedure "Replacing a FabricPool mirror on a MetroCluster configuration" in the Disk and Aggregates Power Guide.

Verifying licenses on the replaced nodes

You must install new licenses for the replacement nodes if the impaired nodes were using ONTAP features that require a standard (node-locked) license. For features with standard licenses, each node in the cluster should have its own key for the feature.

About this task

Until you install license keys, features requiring standard licenses continue to be available to the replacement node. However, if the impaired node was the only node in the cluster with a license for the feature, no configuration changes to the feature are allowed. Also, using unlicensed features on the node might put you out of compliance with your license agreement, so you should install the replacement license key or keys on the replacement node as soon as possible.

The licenses keys must be in the 28-character format.

You have a 90-day grace period in which to install the license keys. After the grace period, all old licenses are invalidated. After a valid license key is installed, you have 24 hours to install all of the keys before the grace period ends.

> ⓘ If all nodes at a site have been replaced (a single node in the case of a two-node MetroCluster configuration), license keys must be installed on the replacement node or nodes prior to switchback.

Steps

1. Identify the licenses on the node:

   `license show`

   The following example displays the information about licenses in the system:

```
cluster_B::>  license show
         (system license show)

Serial Number: 1-80-00050
Owner: site1-01
Package           Type       Description             Expiration
-------          -------     -------------           -----------
Base             license     Cluster Base License        -
NFS              site        NFS License                 -
CIFS             site        CIFS License                -
iSCSI            site        iSCSI License               -
FCP              site        FCP License                 -
FlexClone        site        FlexClone License           -

6 entries were displayed.
```

2. Verify that the licenses are good for the node after switchback:

   `metrocluster check license show`

   The following example displays the licenses that are good for the node:

```
cluster_B::> metrocluster check license show

Cluster           Check                            Result
-------           -------                          -------------
Cluster_B         negotiated-switchover-ready      not-applicable
NFS               switchback-ready                 not-applicable
CIFS              job-schedules                    ok
iSCSI             licenses                         ok
FCP               periodic-check-enabled           ok
```

3. If you need new license keys, obtain replacement license keys on the NetApp Support Site in the My Support section under Software licenses.

   ⓘ The new license keys that you require are automatically generated and sent to the email address on file. If you fail to receive the email with the license keys within 30 days, you should contact technical support.

4. Install each license key:

```
system license add -license-code license-key, license-key…+
```

5. Remove the old licenses, if desired:
   a. Check for unused licenses:

      ```
      license clean-up -unused -simulate
      ```

   b. If the list looks correct, remove the unused licenses:

      ```
      license clean-up -unused
      ```

Performing a switchback

After you heal the MetroCluster configuration, you can perform the MetroCluster switchback operation. The MetroCluster switchback operation returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the disaster site active and serving data from the local disk pools.

Before you begin

- The disaster cluster must have successfully switched over to the surviving cluster.
- Healing must have been performed on the data and root aggregates.
- The surviving cluster nodes must not be in the HA failover state (all nodes must be up and running for each HA pair).
- The disaster site controller modules must be completely booted and not in the HA takeover mode.
- The root aggregate must be mirrored.
- The Inter-Switch Links (ISLs) must be online.
- Any required licenses must be installed on the system.

Steps

1. Confirm that all nodes are in the enabled state:

   ```
   metrocluster node show
   ```

   The following example displays the nodes that are in the enabled state:

```
cluster_B::>  metrocluster node show

DR                          Configuration  DR
Group Cluster Node          State          Mirroring Mode
----- ------- ----------- -------------- --------- --------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots completed
              node_A_2    configured     enabled   heal roots completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Confirm that resynchronization is complete on all SVMs:

   `metrocluster vserver show`

3. Verify that any automatic LIF migrations being performed by the healing operations have been successfully completed:

   `metrocluster check lif show`

4. Perform the switchback by running the `metrocluster switchback` command from any node in the surviving cluster.
5. Check the progress of the switchback operation:

   `metrocluster show`

   The switchback operation is still in progress when the output displays "waiting-for-switchback":

```
cluster_B::> metrocluster show
Cluster                    Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B          Configuration state configured
                           Mode                switchover
                           AUSO Failure Domain -
Remote: cluster_A          Configuration state configured
                           Mode                waiting-for-switchback
                           AUSO Failure Domain -
```

   The switchback operation is complete when the output displays "normal":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

If a switchback takes a long time to finish, you can check on the status of in-progress baselines by using the the following command at the advanced privilege level:

`metrocluster config-replication resync-status show`

6. Reestablish any SnapMirror or SnapVault configurations.

   In ONTAP 8.3, you need to manually reestablish a lost SnapMirror configuration after a MetroCluster switchback operation. In ONTAP 9.0 and later, the relationship is reestablished automatically.

Verifying a successful switchback

After performing the switchback, you want to confirm that all aggregates and storage virtual machines (SVMs) are switched back and online.

Steps

1. Verify that the switched-over data aggregates are switched back:

   `storage aggregate show`

   In the following example, aggr_b2 on node B2 has switched back:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

If the disaster site included unmirrored aggregates and the unmirrored aggregates are no longer present, the aggregate might show up with a state of "unknown" in the output of the storage aggregate show command. Contact technical support to remove the out-of-date entries for the unmirrored aggregates.

2. Verify that all sync-destination SVMs on the surviving cluster are dormant (showing an Admin State of "stopped") and the sync-source SVMs on the disaster cluster are up and running:

```
vserver show -subtype sync-source
```

```
node_B_1::> vserver show -subtype sync-source
                              Admin      Root
Name    Name
Vserver     Type    Subtype    State      Volume     Aggregate
Service Mapping
----------- ------- ---------- ---------- ---------- ----------
------- -------
...
vs1a        data    sync-source
                              running    vs1a_vol   node_B_2
file    file

aggr_b2

node_A_1::> vserver show -subtype sync-destination
                              Admin      Root
Name    Name
Vserver            Type    Subtype    State      Volume     Aggregate
Service Mapping
-----------        ------- ---------- ---------- ---------- ----------
------- -------
...
cluster_A-vs1a-mc  data    sync-destination
                                     stopped    vs1a_vol   sosb_
file    file

aggr_b2
```

Sync-destination aggregates in the MetroCluster configuration have the suffix "-mc" automatically appended to their name to help identify them.

3. Confirm that the switchback operations succeeded by using the `metrocluster operation show` command.

If the command output shows…	Then…
That the switchback operation state is successful.	The switchback process is complete and you can proceed with operation of the system.
That the switchback operation or switchback-continuation-agent operation is partially successful.	Perform the suggested fix provided in the output of the metrocluster operation show command.

After you finish

You must repeat the previous sections to perform the switchback in the opposite direction. If site_A did a switchover of site_B, have site_B do a switchover of site_A.

Mirroring the root aggregates of the replacement nodes

If disks were replaced, you must mirror the root aggregates of the new nodes on the disaster site.

Steps

1. On the disaster site, identify the aggregates which are not mirrored:

   `storage aggregate show`

   ```
   cluster_A::> storage aggregate show

   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_A_1_aggr0
               1.49TB   74.12GB   95% online       1 node_A_1
   raid4,

   normal
   node_A_2_aggr0
               1.49TB   74.12GB   95% online       1 node_A_2
   raid4,

   normal
   node_A_1_aggr1
               1.49TB   74.12GB   95% online       1 node_A_1         raid
   4, normal

   mirrored
   node_A_2_aggr1
               1.49TB   74.12GB   95% online       1 node_A_2         raid
   4, normal

   mirrored
   4 entries were displayed.

   cluster_A::>
   ```

2. Mirror one of the root aggregates:

   `storage aggregate mirror -aggregate root-aggregate`

   The following example shows how the command selects disks and prompts for confirmation when mirroring the aggregate.

```
cluster_A::> storage aggregate mirror -aggregate node_A_2_aggr0

Info: Disks would be added to aggregate "node_A_2_aggr0" on node
"node_A_2" in
      the following manner:

      Second Plex

        RAID Group rg0, 3 disks (block checksum, raid4)
          Position   Disk                        Type
Size
          ---------- ------------------------- ----------
---------------
          parity     2.10.0                      SSD
-
          data       1.11.19                     SSD
894.0GB
          data       2.10.2                      SSD
894.0GB

      Aggregate capacity available for volume use would be 1.49TB.

Do you want to continue? {y|n}: y

cluster_A::>
```

3. Verify that mirroring of the root aggregate is complete:

   `storage aggregate show`

   The following example shows that the root aggregates are mirrored.

```
cluster_A::> storage aggregate show

Aggregate     Size Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ -----------
------------
node_A_1_aggr0
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                              mirrored,
                                                              normal
node_A_2_aggr0
            2.24TB   838.5GB   63% online       1 node_A_2    raid4,
                                                              mirrored,
                                                              normal
node_A_1_aggr1
            1.49TB   74.12GB   95% online       1 node_A_1    raid4,
                                                              mirrored,
                                                              normal
node_A_2_aggr1
            1.49TB   74.12GB   95% online       1 node_A_2    raid4
                                                              mirrored,
                                                              normal
4 entries were displayed.

cluster_A::>
```

4. Repeat these steps for the other root aggregates.

   Any root aggregate that does not have a status of mirrored must be mirrored.

Reconfiguring the ONTAP Mediator service (MetroCluster IP configurations)

If you have a MetroCluster IP configuration that was configured with the ONTAP Mediator service, you must remove and reconfigure the association with the mediator.

Before you begin

- You must have the IP address and username and password for the ONTAP Mediator service.
- The ONTAP Mediator service must be configured and operating on the Linux host.

Steps

1. Remove the existing ONTAP Mediator configuration:

   `metrocluster configuration-settings mediator remove`

2. Reconfigure the ONTAP Mediator configuration:

   `metrocluster configuration-settings mediator add -mediator-address mediator-`

IP-address

Verifying the health of the MetroCluster configuration

You should check the health of the MetroCluster configuration to verify proper operation.

Steps

1. Check that the MetroCluster is configured and in normal mode on each cluster:

   `metrocluster show`

   ```
   cluster_A::> metrocluster show
   Cluster                    Entry Name          State
   ------------------------- ------------------- -----------
    Local: cluster_A         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   Remote: cluster_B         Configuration state configured
                             Mode                normal
                             AUSO Failure Domain auso-on-cluster-disaster
   ```

2. Check that mirroring is enabled on each node:

   `metrocluster node show`

   ```
   cluster_A::> metrocluster node show
   DR                            Configuration  DR
   Group Cluster Node            State          Mirroring Mode
   ----- ------- -------------- -------------- ---------
   --------------------
   1     cluster_A
                 node_A_1       configured     enabled   normal
         cluster_B
                 node_B_1       configured     enabled   normal
   2 entries were displayed.
   ```

3. Check that the MetroCluster components are healthy:

   `metrocluster check run`

```
cluster_A::> metrocluster check run

Last Checked On: 10/1/2014 16:03:37

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command
or sub-commands in "metrocluster check" directory for detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

4. Check that there are no health alerts:

   `system health alert show`

5. Simulate a switchover operation:

   a. From any node's prompt, change to the advanced privilege level:

      `set -privilege advanced`

      You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

   b. Perform the switchover operation with the `-simulate` parameter:

      `metrocluster switchover -simulate`

   c. Return to the admin privilege level:

      `set -privilege admin`

6. For MetroCluster IP configurations using the ONTAP Mediator service, confirm that the Mediator service is up and operating.

   a. Check that the Mediator disks are visible to the system:

      `storage failover mailbox-disk show`

      The following example shows that the mailbox disks have been recognized.

```
node_A_1::*> storage failover mailbox-disk show
                  Mailbox
Node              Owner     Disk    Name        Disk UUID
-------------     ------   -----   -----       ----------------
sti113-vsim-ucs626g
.
.
     local     0m.i2.3L26
7BBA77C9:AD702D14:831B3E7E:0B0730EE:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i2.3L27
928F79AE:631EA9F9:4DCB5DE6:3402AC48:00000000:00000000:00000000:000000
00:00000000:00000000
     local     0m.i1.0L60
B7BCDB3C:297A4459:318C2748:181565A3:00000000:00000000:00000000:000000
00:00000000:00000000
.
.
.
     partner   0m.i1.0L14
EA71F260:D4DD5F22:E3422387:61D475B2:00000000:00000000:00000000:000000
00:00000000:00000000
     partner   0m.i2.3L64
4460F436:AAE5AB9E:D1ED414E:ABF811F7:00000000:00000000:00000000:000000
00:00000000:00000000
28 entries were displayed.
```

b. Change to the advanced privilege level:

```
set -privilege advanced
```

c. Check that the mailbox LUNs are visible to the system:

```
storage iscsi-initiator show
```

The output will show the presence of the mailbox LUNs:

```
Node    Type       Label      Target Portal     Target Name
Admin/Op
----    ----       --------   ---------    ---------
--------------------------------       --------
.
.
.
.node_A_1
               mailbox
                     mediator 172.16.254.1    iqn.2012-
05.local:mailbox.target.db5f02d6-e3d3    up/up
.
.
.
17 entries were displayed.
```

d. Return to the administrative privilege level:

```
set -privilege admin
```

Recovering from a non-controller failure

After the equipment at the disaster site has undergone any required maintenance or replacement, but no controllers were replaced, you can begin the process of returning the MetroCluster configuration to a fully redundant state. This includes healing the configuration (first the data aggregates and then the root aggregates) and performing the switchback operation.

Before you begin

- All MetroCluster hardware in the disaster cluster must be functional.
- The overall MetroCluster configuration must be in switchover.
- In a fabric-attached MetroCluster configuration, the ISL must be up and operating between the MetroCluster sites.

Healing the configuration in a MetroCluster FC configuration

Following a switchover, you must perform the healing operations in specific order to restore MetroCluster functionality.

Before you begin

- Switchover must have been performed and the surviving site must be serving data.
- Nodes on the disaster site must be halted or remain powered off.

  They must not be fully booted during the healing process.

- Storage at the disaster site must be accessible (shelves are powered up, functional, and accessible).
- In fabric-attached MetroCluster configurations, inter-switch links (ISLs) must be up and operating.
- In four-node MetroCluster configurations, nodes in the surviving site must not be in HA failover state (all nodes must be up and running for each HA pair).

About this task

The healing operation must first be performed on the data aggregates, and then on the root aggregates.

Healing the data aggregates

You must heal the data aggregates after repairing and replacing any hardware on the disaster site. This process resynchronizes the data aggregates and prepares the (now repaired) disaster site for normal operation. You must heal the data aggregates prior to healing the root aggregates.

About this task

The following example shows a forced switchover, where you bring the switched-over aggregate online. All configuration updates in the remote cluster successfully replicate to the local cluster. You power up the storage on the disaster site as part of this procedure, but you do not and must not power up the controller modules on the disaster site.

Steps

1. Verify that switchover was completed:

   `metrocluster operation show`

   ```
   controller_A_1::> metrocluster operation show
     Operation: switchover
         State: successful
    Start Time: 7/25/2014 20:01:48
      End Time: 7/25/2014 20:02:14
        Errors: -
   ```

2. Resynchronize the data aggregates by running the following command from the surviving cluster:

   `metrocluster heal -phase aggregates`

   ```
   controller_A_1::> metrocluster heal -phase aggregates
   [Job 130] Job succeeded: Heal Aggregates is successful.
   ```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `--override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

3. Verify that the operation has been completed:

   `metrocluster operation show`

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2014 18:45:55
   End Time: 7/25/2014 18:45:56
     Errors: -
```

4. Check the state of the aggregates:

   `storage aggregate show` command.

```
controller_A_1::> storage aggregate show
Aggregate Size     Available Used% State   #Vols  Nodes        RAID
Status
--------- -------- --------- ----- ------- ------ ------------
------------
...
aggr_b2   227.1GB  227.1GB   0%    online  0      mcc1-a2      raid_dp,
mirrored, normal...
```

5. If storage has been replaced at the disaster site, you might need to remirror the aggregates.

Healing the root aggregates after a disaster

After the data aggregates have been healed, you must heal the root aggregates in preparation for the switchback operation.

Before you begin

The data aggregates phase of the MetroCluster healing process must have been completed successfully.

Steps

1. Switch back the mirrored aggregates:

   `metrocluster heal -phase root-aggregates`

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

   If the healing is vetoed, you have the option of reissuing the `metrocluster heal` command with the `--override-vetoes` parameter. If you use this optional parameter, the system overrides any soft vetoes that prevent the healing operation.

2. Ensure that the heal operation is complete by running the following command on the destination cluster:

   `metrocluster operation show`

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2014 20:54:41
   End Time: 7/29/2014 20:54:42
     Errors: -
```

3. Power up each controller module on the disaster site.
4. After nodes are booted, verify that the root aggregates are mirrored.

   If both plexes are present, any resynchronization will start automatically. If one plex has failed, that plex must be destroyed and the mirror recreated using the following command to reestablish the mirror relationship.

   `storage aggregate mirror -aggregate <aggregate-name>`

Verifying that your system is ready for a switchback

If your system is already in the switchover state, you can use the `-simulate` option to preview the results of a switchback operation.

Steps

1. Simulate the switchback operation:
   a. From either surviving node’s prompt, change to the advanced privilege level:

      `set -privilege advanced`

      You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

   b. Perform the switchback operation with the `-simulate` parameter:

      `metrocluster switchback -simulate`

   c. Return to the admin privilege level:

      `set -privilege admin`

2. Review the output that is returned.

   The output shows whether the switchback operation would run into errors.

Example of verification results

The following example shows the successful verification of a switchback operation:

```
cluster4::*> metrocluster switchback -simulate
  (metrocluster switchback)
[Job 130] Setting up the nodes and cluster components for the switchback
operation...DBG:backup_api.c:327:backup_nso_sb_vetocheck : MetroCluster
Switch Back
[Job 130] Job succeeded: Switchback simulation is successful.

cluster4::*> metrocluster op show
  (metrocluster operation show)
  Operation: switchback-simulate
      State: successful
 Start Time: 5/15/2014 16:14:34
   End Time: 5/15/2014 16:15:04
     Errors: -

cluster4::*> job show -name Me*
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
130    MetroCluster Switchback
                            cluster4
                                       cluster4-01
                                                      Success
       Description: MetroCluster Switchback Job - Simulation
```

Performing a switchback

After you heal the MetroCluster configuration, you can perform the MetroCluster switchback operation. The MetroCluster switchback operation returns the configuration to its normal operating state, with the sync-source storage virtual machines (SVMs) on the disaster site active and serving data from the local disk pools.

Before you begin

- The disaster cluster must have successfully switched over to the surviving cluster.
- Healing must have been performed on the data and root aggregates.
- The surviving cluster nodes must not be in the HA failover state (all nodes must be up and running for each HA pair).
- The disaster site controller modules must be completely booted and not in the HA takeover mode.
- The root aggregate must be mirrored.
- The Inter-Switch Links (ISLs) must be online.
- Any required licenses must be installed on the system.

Steps

1. Confirm that all nodes are in the enabled state:

```
metrocluster node show
```

The following example displays the nodes that are in the "enabled" state:

```
cluster_B::>  metrocluster node show

DR                          Configuration  DR
Group Cluster Node          State          Mirroring Mode
----- ------- ----------- -------------- --------- --------------------
1     cluster_A
              node_A_1    configured     enabled   heal roots completed
              node_A_2    configured     enabled   heal roots completed
      cluster_B
              node_B_1    configured     enabled   waiting for
switchback recovery
              node_B_2    configured     enabled   waiting for
switchback recovery
4 entries were displayed.
```

2. Confirm that resynchronization is complete on all SVMs:

```
metrocluster vserver show
```

3. Verify that any automatic LIF migrations being performed by the healing operations have been successfully completed:

```
metrocluster check lif show
```

4. Perform the switchback by running the following command from any node in the surviving cluster.

```
metrocluster switchback
```

5. Check the progress of the switchback operation:

```
metrocluster show
```

The switchback operation is still in progress when the output displays "waiting-for-switchback":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                switchover
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                waiting-for-switchback
                          AUSO Failure Domain -
```

The switchback operation is complete when the output displays "normal":

```
cluster_B::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
Remote: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain -
```

If a switchback takes a long time to finish, you can check on the status of in-progress baselines by using the following command at the advanced privilege level.

`metrocluster config-replication resync-status show`

6. Reestablish any SnapMirror or SnapVault configurations.

   In ONTAP 8.3, you need to manually reestablish a lost SnapMirror configuration after a MetroCluster switchback operation. In ONTAP 9.0 and later, the relationship is reestablished automatically.

Verifying a successful switchback

After performing the switchback, you want to confirm that all aggregates and storage virtual machines (SVMs) are switched back and online.

Steps

1. Verify that the switched-over data aggregates are switched back:

   `storage aggregate show`

   In the following example, aggr_b2 on node B2 has switched back:

```
node_B_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 node_B_2   raid_dp,

mirrored,

normal

node_A_1::> aggr show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2          -         -     - unknown      - node_A_1
```

If the disaster site included unmirrored aggregates and the unmirrored aggregates are no longer present, the aggregate might show up with a state of "unknown" in the output of the `storage aggregate show` command. Contact technical support to remove the out-of-date entries for the unmirrored aggregates.

2. Verify that all sync-destination SVMs on the surviving cluster are dormant (showing an admin state of "stopped") and the sync-source SVMs on the disaster cluster are up and running:

```
vserver show -subtype sync-source
```

```
node_B_1::> vserver show -subtype sync-source
                              Admin      Root
Name    Name
Vserver     Type    Subtype    State      Volume     Aggregate
Service Mapping
----------- ------- ---------- ---------- ---------- ----------
------- -------
...
vs1a        data    sync-source
                              running    vs1a_vol   node_B_2
file    file

aggr_b2

node_A_1::> vserver show -subtype sync-destination
                              Admin      Root
Name    Name
Vserver            Type    Subtype    State      Volume     Aggregate
Service Mapping
-----------        ------- ---------- ---------- ---------- ----------
------- -------
...
cluster_A-vs1a-mc  data    sync-destination
                                     stopped    vs1a_vol   sosb_
file    file

aggr_b2
```

Sync-destination aggregates in the MetroCluster configuration have the suffix "-mc" automatically appended to their name to help identify them.

3. Confirm that the switchback operations succeeded:

```
metrocluster operation show
```

If the command output shows…	Then…
That the switchback operation state is successful.	The switchback process is complete and you can proceed with operation of the system.
That the switchback operation or `switchback-continuation-agent` operation is partially successful.	Perform the suggested fix provided in the output of the `metrocluster operation show` command.

After you finish

You must repeat the previous sections to perform the switchback in the opposite direction. If site_A did a switchover of site_B, have site_B do a switchover of site_A.

Deleting stale aggregate listings after switchback

In some circumstances after switchback, you might notice the presence of *stale* aggregates. Stale aggregates are aggregates that have been removed from ONTAP, but whose information remains recorded on disk. Stale aggregates are displayed with the `nodeshell aggr status -r` command but not with the `storage aggregate show` command. You can delete these records so that they no longer appear.

About this task

Stale aggregates can occur if you relocated aggregates while the MetroCluster configuration was in switchover. For example:

1. Site A switches over to Site B.
2. You delete the mirroring for an aggregate and relocate the aggregate from node_B_1 to node_B_2 for load balancing.
3. You perform aggregate healing.

At this point a stale aggregate appears on node_B_1, even though the actual aggregate has been deleted from that node. This aggregate appears in the output from the `nodeshell aggr status -r` command. It does not appear in the output of the `storage aggregate show` command.

1. Compare the output of the following commands:

   ```
   storage aggregate show
   ```

   ```
   run local aggr status -r
   ```

   Stale aggregates appear in the `run local aggr status -r` output but not in the `storage aggregate show` output. For example, the following aggregate might appear in the `run local aggr status -r` output:

```
Aggregate aggr05 (failed, raid_dp, partial) (block checksums)
Plex /aggr05/plex0 (offline, failed, inactive)
  RAID group /myaggr/plex0/rg0 (partial, block checksums)

 RAID Disk Device  HA  SHELF BAY CHAN Pool Type  RPM  Used (MB/blks)
Phys (MB/blks)
 --------- ------  ------------- ---- ---- ----  ----- --------------
--------------
 dparity   FAILED          N/A                        82/ -
 parity    0b.5    0b    -   -   SA:A   0 VMDISK  N/A 82/169472
88/182040
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 data      FAILED          N/A                        82/ -
 Raid group is missing 7 disks.
```

2. Remove the stale aggregate:

   a. From either node’s prompt, change to the advanced privilege level:

      ```
      set -privilege advanced
      ```

      You need to respond with `y` when prompted to continue into advanced mode and see the advanced mode prompt (*>).

   b. Remove the stale aggregate:

      ```
      aggregate remove-stale-record -aggregate aggregate_name
      ```

   c. Return to the admin privilege level:

      ```
      set -privilege admin
      ```

3. Confirm that the stale aggregate record was removed:

   ```
   run local aggr status -r
   ```

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

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.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Machine translation

See important information about localized content at netapp.com