



ONTAP 9 Documentation

ONTAP 9

NetApp

May 31, 2021

This PDF was generated from <https://docs.netapp.com/us-en/ontap/index.html> on May 31, 2021. Always check docs.netapp.com for the latest.

Table of Contents

ONTAP 9 Documentation	1
About ONTAP System Manager	1
Key concepts	3
Configure ONTAP	5
Decide whether to use the ONTAP CLI for cluster setup	5
Set up the cluster with the ONTAP CLI	5
Upgrade ONTAP	18
What version of ONTAP can I upgrade to?	18
How to plan your upgrade	19
What to check before upgrading	24
Download and install the ONTAP software image	47
Which upgrade method should I use?	50
What to do after upgrading	92
Revert ONTAP	105
Revert paths	105
What should I read before I revert?	106
Things to verify before you revert	107
Pre-revert checks	113
Download and install the ONTAP software image	120
Revert an ONTAP cluster	122
Things to verify after revert	125
ONTAP 9 Network Management Documentation	134
Viewing and managing your network	134
Downloading network data for reporting	136
Set up NAS path failover (ONTAP 9.8 and later CLI)	136
Set up NAS path failover (ONTAP 9.0 - 9.7 CLI)	158
ONTAP 9 Networking Reference	178
High Availability	329
How hardware-assisted takeover works	329
How automatic takeover and giveback works	331
Automatic takeover commands	334
Automatic giveback commands	335
Commands for monitoring an HA pair	338
Commands for enabling and disabling storage failover	342
Documentation for the SnapMirror Business Continuity solution	343
Introduction	343
Planning	345
Installation and setup	350
Administration	355
Troubleshooting	364
Provision SAN storage	373
SAN overview	373
Provision SAN storage for VMware datastores	374

Provision SAN storage for Linux servers	375
Provision SAN storage for Windows servers	376
Create nested igroup	377
Map igrups to multiple LUNs	377
SnapMirror Business Continuity	378
Provision NVMe storage	381
NVMe overview	381
Provision NVMe storage for SUSE Linux	381
Provision NAS storage	383
NAS overview for ONTAP System Manager	383
Provision NAS storage for VMware datastores	383
Provision NAS storage for home directories	384
Provision NAS storage for Linux servers using NFS	384
Manage access using export policies	385
Provision NAS storage for Windows servers using SMB/CIFS	385
Provision NAS storage for both Windows and Linux using both NFS and SMB/CIFS	385
Secure client access with Kerberos	386
Provide client access with name services	388
Provision NAS storage for large file systems using FlexGroup volumes	388
Manage directories and files	390
Monitor volume usage with ONTAP File System Analytics	390
Monitor NFS active clients	393
Improve performance for multiple clients with FlexCache	394
Enable NAS storage	395
Provision object storage	399
ONTAP S3 overview for System Manager	399
Enable an S3 server on a storage	400
Provision buckets	400
Add S3 users and groups	401
Manage user access to buckets	401
Manage user access to S3-enabled storage VMs	402
Manage resources using quotas	404
Quota overview	404
Set quotas to limit resource use	404
Maximize security	405
Security overview for System Manager	405
Set up multifactor authentication	406
Control administrator access	407
Encrypt stored data using software-based encryption	408
Encrypt stored data using self-encrypting drives	408
Diagnose and correct file access issues	409
Protect data	410
Data protection overview	410
Create custom data protection policies	410
Configure Snapshot copies	411

Recover from Snapshot copies	411
Prepare for mirroring and vaulting	411
Configure mirrors and vaults	412
Configure storage VM disaster recovery	413
Serve data from a SnapMirror destination	413
Resynchronize a protection relationship	414
Restore a volume from an earlier Snapshot copy	414
Restore to a new volume	414
Reverse Resynchronizing a Protection Relationship	415
Reactivate a source storage VM	415
Resynchronize a destination storage VM	415
Back up to the cloud	416
Extend to the cloud	418
Cloud overview	418
Add a connection to the cloud	419
Tier data to cloud	419
Tier data to local bucket	420
Create tags for tiering objects	421
Enable inactive data reporting	421
Back up data using the Cloud Backup Service	421
Manage the connection to the Cloud Backup Service	424
View cluster performance	426
Cluster performance overview with System Manager	426
View performance on cluster dashboard	426
Identify hot volumes and other objects	427
Monitor cluster performance using System Manager	427
Monitor cluster performance with Unified Manager	427
Monitor cluster performance with Cloud Insights	428
Day-to-day administration overview	430
Administration overview with System Manager	430
Search, filter, and sort information in System Manager	431
Enable new features by adding license keys	433
Reboot, shut down, take over, and give back nodes	433
View hardware configurations to determine problems	433
View and submit support cases	436
Manage MetroCluster sites	436
Clone volumes and LUNs for testing	444
Modify QoS	445
Update firmware	445
Manage storage	447
Rest API	456
REST API log overview	456
Accessing the REST API log	456
Getting more information	459
Legal notices	460

Copyright	460
Trademarks	460
Patents	460
Privacy policy	460

ONTAP 9 Documentation

This is the new home for ONTAP 9 documentation. It focuses on setting up and managing your ONTAP storage with the most current versions of ONTAP System Manager.

We also provide documentation links for managing your storage with:

- ONTAP CLI
- Legacy OnCommand System Manager

If you are managing your ONTAP storage with the ONTAP REST API, you can get started [here](#).

About ONTAP System Manager

ONTAP System Manager (formerly OnCommand System Manager) is a simple and versatile product that enables you to easily configure and manage ONTAP clusters. System Manager simplifies common storage tasks such as creating volumes, LUNs, qtrees, shares, and exports, which saves time and helps prevent errors.



Beginning with ONTAP 9.7, a totally redesigned ONTAP System Manager simplifies ONTAP management with an intuitive graphical user interface that offers:

- Fast, simple configuration

Simplified workflows for ONTAP setup and management of common tasks.

- Smart defaults

Enable you to create best-practice configurations based on proven deployments.

- Extensive administrative capabilities

Easily configure and provision storage for file sharing, application and database workloads.

- Integrated management

System Manager comes bundled with the ONTAP 9 platform, eliminating the need for a separate installation. A new dashboard that shows key cluster status and performance on one screen.

For information on previous versions of System Manager, see the [ONTAP 9 Documentation Center](#).

Key concepts

NetApp ONTAP is NetApp's proven data management software. You can run ONTAP in your data center on NetApp-engineered hardware, on your commodity hardware, or in any of the major public clouds.

Starting with ONTAP 9.7, you can manage your system with the all-new ONTAP System Manager interface. This web-based interface gets you up and running with just a few clicks.

ONTAP System Manager gives you a clear visual of the status of your cluster and guides you on the best ways to achieve your storage goals.

If you are familiar with a previous version of ONTAP, you will feel right at home. There are a few terminology changes with ONTAP System Manager that you should be aware of.

- **Local tier** – a set of physical solid-state drives or hard-disk drives you store your data on. You might know these as aggregates. In fact, if you use the ONTAP CLI, you will still see the term *aggregate* used to represent a local tier.
- **Cloud tier** – storage in the cloud used by ONTAP when you want to have some of your data off premises for one of several reasons. If you are thinking of the cloud part of a FabricPool, you've already figured it out. And if you are using a StorageGRID system, your cloud might not be off premises at all. (A cloud like experience on premises is called a *private cloud*.)
- **Storage VM** – a virtual machine running within ONTAP that provides storage and data services to your clients. You might know this as an *SVM* or a *vserver*.
- **Network interface** - an address and properties assigned to a physical network port. You might know this as a *logical interface (LIF)*.

If you are new to ONTAP, here are a few other concepts that will get you up to speed.

- **Cluster** – that's the big picture. A cluster is made up of one or more nodes. Think of nodes as computers that specialize in data management and storage. You can add nodes to your cluster as your needs grow, or you can replace smaller nodes with bigger ones. All without interrupting access to your data, of course.
- **Snapshot copies** – these are instant copies of your data that you can use to undo a mistake, move or back up to cloud, mirror to another cluster, or even copy to tape. Without interruption to your clients. And who can afford downtime?
- **Data protection** - the protection features you use depend on what you need to protect against and how long you can wait to recover if something goes wrong. ONTAP offers synchronous and asynchronous mirroring and more.
- **HA pair** – speaking of avoiding downtime, the high-availability pair is the basic unit of an ONTAP cluster. It's made up of two partner nodes that can take over for each other. Say you want to upgrade to the latest version of ONTAP to get a great new data management feature. Just have the partner take over a node's client load, upgrade that client, and then give the load back. Repeat for the partner node and you have just upgraded without any disruption.
- **Storage efficiency** – disks cost money (real money!), but storage efficiency lets you store more data in less space. And that saves real money and makes you a data hero. You can use any or all of ONTAP's compression, deduplication, and compaction features. We're sure you already know what compression is. Deduplication identifies multiple copies of the same data and replaces the duplicates with pointers to a single copy. Compaction puts multiple small files into a single block of storage, filling in what would otherwise be wasted space.

- **Security** – security is integral to ONTAP data management software. ONTAP helps you out in many ways, such as using multifactor authentication for administrators, encrypting data on disk and in flight, and using antivirus tools to protect Windows files.
- **Volumes** – are exactly what you think volumes are. They're containers to store files. You can export volumes to Linux clients, share volumes with Windows clients, or even do both at the same time with the same files.
- **LUNs** – the basic unit of SAN. That's Fibre Channel and iSCSI. In a SAN environment, ONTAP provides virtual disks to clients instead of files. Database administrators often want virtual disks that they can manage at a low level or apply a specialized file system to. Many ONTAP systems, but not all, can serve data to SAN clients.
- **NVMe namespaces** – the future of flash storage. The NVMe protocol is optimized for SSD-based storage, and it is really fast. NVMe is a flavor of SAN, but the basic unit of storage is called a *namespace* instead of a LUN.

So now you know the basics of ONTAP and you're ready to get to work. Read the sections that follow to learn how to set up and manage your cluster with System Manager.

If you want to learn even more, check out the ONTAP [Concepts Guide](#). Join a NetApp community. And just click around to see what else is there.

Configure ONTAP

Decide whether to use the ONTAP CLI for cluster setup

While you can set up new clusters with the ONTAP CLI, NetApp recommends that you use ONTAP System Manager whenever possible to simplify the cluster setup process. Use these procedures only if your version of ONTAP System Manager does not support initial cluster setup for your planned ONTAP deployment.

You should be aware of the following System Manager support requirements:

- Cluster setup is supported only for single nodes and HA pairs
- When you set up node management manually using the CLI, System Manager supports only IPv4 and does not support IPv6. However, if you launch System Manager after completing your hardware setup using DHCP with an auto assigned IP address and with Windows discovery, System Manager can configure an IPv6 management address.

In ONTAP 9.6 and earlier, System Manager does not support deployments that require IPv6 networking.

- MetroCluster setup support is for MetroCluster IP configurations with two nodes at each site.

In ONTAP 9.7 and earlier, System Manager does not support new cluster setup for MetroCluster configurations.

If you are configuring a FlexArray on non-NetApp disks, you need to use the ONTAP CLI to configure root volumes on the array LUNs, and then use the Cluster Setup wizard to set up your cluster.

For more information, see the [FlexArray Virtualization Installation and Requirements Reference](#).

Before completing any of these procedures, you should have installed, cabled and powered on your new storage system according to the installation and setup instructions for your platform model.

See the [AFF and FAS Documentation Center](#).

Set up the cluster with the ONTAP CLI

Setting up the cluster involves gathering the information needed to configure setting up each node, creating the cluster on the first node, and joining any remaining nodes to the cluster.

Get started by gathering all the relevant information in the cluster setup worksheets.

Cluster setup worksheets

The cluster setup worksheet enables you to record the values that you need during the cluster setup process. If a default value is provided, you can use that value or else enter your own.

System defaults

The system defaults are the default values for the private cluster network. It is best to use these default values. However, if they do not meet your requirements, you can use the table to record your own values.



For clusters configured to use network switches, each cluster switch must use the 9000 MTU size.

Types of information	Your values
Private cluster network ports	
Cluster network netmask	
Cluster interface IP addresses (for each cluster network port on each node)	
The IP addresses for each node must be on the same subnet.	

Cluster information

Types of information	Your values
Cluster name The name must begin with a letter, and it must be fewer than 44 characters. The name can include the following special characters: • - _	

Feature license keys

You can find license keys for your initial or add-on software orders at the NetApp Support Site under **My Support > Software Licenses**.

Types of information	Your values
Feature license keys	

Admin storage virtual machine (SVM)

Types of information	Your values
<p>Cluster administrator password</p> <p>The password for the admin account that the cluster requires before granting cluster administrator access to the console or through a secure protocol.</p> <p> For security purposes, recording passwords in this worksheet is not recommended.</p> <p>The default rules for passwords are as follows:</p> <ul style="list-style-type: none"> • A password must be at least eight characters long. • A password must contain at least one letter and one number. 	
<p>Cluster management interface port</p> <p>The physical port that is connected to the data network and enables the cluster administrator to manage the cluster.</p>	
<p>Cluster management interface IP address</p> <p>A unique IPv4 or IPv6 address for the cluster management interface. The cluster administrator uses this address to access the admin SVM and manage the cluster. Typically, this address should be on the data network.</p> <p>You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.</p> <p>Example: 192.0.2.66</p>	
<p>Cluster management interface netmask (IPv4)</p> <p>The subnet mask that defines the range of valid IPv4 addresses on the cluster management network.</p> <p>Example: 255.255.255.0</p>	

Types of information	Your values
<p>Cluster management interface netmask length (IPv6)</p> <p>If the cluster management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the cluster management network.</p> <p>Example: 64</p>	
<p>Cluster management interface default gateway</p> <p>The IP address for the router on the cluster management network.</p>	
<p>DNS domain name</p> <p>The name of your network's DNS domain.</p> <p>The domain name must consist of alphanumeric characters. To enter multiple DNS domain names, separate each name with either a comma or a space.</p>	
<p>Name server IP addresses</p> <p>The IP addresses of the DNS name servers. Separate each address with either a comma or a space.</p>	

Node information (for each node in the cluster)

Types of information	Your values
<p>Physical location of the controller (optional)</p> <p>A description of the physical location of the controller. Use a description that identifies where to find this node in the cluster (for example, "Lab 5, Row 7, Rack B").</p>	
<p>Node management interface port</p> <p>The physical port that is connected to the node management network and enables the cluster administrator to manage the node.</p>	

Types of information	Your values
<p>Node management interface IP address</p> <p>A unique IPv4 or IPv6 address for the node management interface on the management network. If you defined the node management interface port to be a data port, then this IP address should be a unique IP address on the data network.</p> <p>You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.</p> <p>Example: 192.0.2.66</p>	
<p>Node management interface netmask (IPv4)</p> <p>The subnet mask that defines the range of valid IP addresses on the node management network.</p> <p>If you defined the node management interface port to be a data port, then the netmask should be the subnet mask for the data network.</p> <p>Example: 255.255.255.0</p>	
<p>Node management interface netmask length (IPv6)</p> <p>If the node management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the node management network.</p> <p>Example: 64</p>	
<p>Node management interface default gateway</p> <p>The IP address for the router on the node management network.</p>	

NTP server information

Types of information	Your values
<p>NTP server addresses</p> <p>The IP addresses of the Network Time Protocol (NTP) servers at your site. These servers are used to synchronize the time across the cluster.</p>	

Create the cluster on the first node

You use the Cluster Setup wizard to create the cluster on the first node. The wizard helps you to configure the cluster network that connects the nodes, create the cluster admin storage virtual machine (SVM), add feature license keys, and create the node management interface for the first node.

1. Power on all the nodes you are adding to the cluster. This is required to enable discovery for your cluster setup.
2. Connect to the console of the first node.

The node boots, and then the Cluster Setup wizard starts on the console.

```
Welcome to the cluster setup wizard....
```

3. Acknowledge the AutoSupport statement.

```
Type yes to confirm and continue {yes}: yes
```



AutoSupport is enabled by default.

4. Follow the instructions on the screen to assign an IP address to the node.
5. If you are using the GUI wizard to perform setup, follow the instructions to complete setup in your web browser. If you are using the CLI wizard to perform setup, press Enter to continue.

```
Use your web browser to complete cluster setup by accessing  
https://10.63.11.29
```

```
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}:
```

6. Create a new cluster: `create`
7. Accept the system defaults or enter your own values.
8. After setup is completed, log in to the cluster and verify that the cluster is active and the first node is healthy by entering the ONTAP CLI command: `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
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the `cluster setup` command.

Join remaining nodes to the cluster

After creating a new cluster, you use the Cluster Setup wizard to join each remaining node to the cluster one at a time. The wizard helps you to configure each node's node management interface.

When you join two nodes in a cluster, you are creating a high availability (HA) pair. If you join 4 nodes, you create two HA pairs. To learn more about HA, see [Learn about HA](#).

You can only join one node to the cluster at a time. When you start to join a node to the cluster, you must complete the join operation for that node, and the node must be part of the cluster before you can start to join the next node.

Best Practice: If you have a FAS2720 with 24 or fewer NL-SAS drives, you should verify that the storage configuration default is set to active/passive to optimize performance.

For more information, see [Setting up an active-passive configuration on nodes using root-data partitioning](#)

1. Log in to the node you plan to join in the cluster.

Cluster Setup wizard starts on the console.

```
Welcome to the cluster setup wizard....
```

2. Acknowledge the AutoSupport statement.



AutoSupport is enabled by default.

```
Type yes to confirm and continue {yes}: yes
```

3. Follow the instructions on the screen to assign an IP address to the node.
4. Join the node to the cluster: `join`
5. Follow the instructions on the screen to set up the node and join it to the cluster.
6. After setup is completed, 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 the cluster:

```
cluster1::> cluster show
Node           Health  Eligibility
-----
cluster1-01    true    true
cluster1-02    true    true
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the cluster setup command.

7. Repeat this task for each remaining node.

Check your cluster with Active IQ Config Advisor

After you have joined all the nodes to your new cluster, you should run Active IQ Config Advisor to validate your configuration and check for common configuration errors.

Config Advisor is a web-based application that you install on your laptop, virtual machine or a server, and works across Windows, Linux, and Mac platforms.

Config Advisor runs a series of commands to validate your installation and check the overall health of the configuration, including the cluster and storage switches.

1. Download and install Active IQ Config Advisor.

[Active IQ Config Advisor](#)

2. Launch Active IQ, and set up a passphrase when prompted.
3. Review your settings and click **Save**.
4. On the **Objectives** page, click **ONTAP Post-Deployment Validation**.
5. Choose either Guided or Expert mode.

If you choose Guided mode, connected switches are discovered automatically.

6. Enter the cluster credentials.
7. (Optional) Click **Form Validate**.
8. To begin collecting data, click **Save & Evaluate**.
9. After data collection is complete, under **Job Monitor > Actions**, view the data collected by clicking **Data View** icon, and view the results by clicking the **Results** icon.
10. Resolve the issues identified by Config Advisor.

Synchronize the system time across the cluster

Synchronizing the time ensures that every node in the cluster has the same time, and prevents CIFS and Kerberos failures.

A Network Time Protocol (NTP) server should be set up at your site. Beginning in ONTAP 9.5, you can set up your NTP server with symmetric authentication.

For more information, see [Managing the cluster time \(cluster administrators only\)](#).

You synchronize the time across the cluster by associating the cluster with one or more NTP servers.

1. Verify that the system time and time zone is set correctly for each node.

All nodes in the cluster should be set to the same time zone.

- a. Use the cluster date show command to display the current date, time, and time zone for each node.

```
cluster1::> cluster date show
Node          Date                  Time zone
-----
cluster1-01   01/06/2015 09:35:15 America/New_York
cluster1-02   01/06/2015 09:35:15 America/New_York
cluster1-03   01/06/2015 09:35:15 America/New_York
cluster1-04   01/06/2015 09:35:15 America/New_York
4 entries were displayed.
```

- b. Use the cluster date modify command to change the date or time zone for all of the nodes.

This example changes the time zone for the cluster to be GMT:

```
cluster1::> cluster date modify -timezone GMT
```

2. Use the cluster time-service ntp server create command to associate the cluster with your NTP server.

- To set up your NTP server without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_name`
- To set up your NTP server with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id`



Symmetric authentication is available beginning in ONTAP 9.5. It is not available in ONTAP 9.4 or earlier.

This example assumes that DNS has been configured for the cluster. If you have not configured DNS, you must specify the IP address of the NTP server:

```
cluster1::> cluster time-service ntp server create -server
ntp1.example.com
```

3. Verify that the cluster is associated with an NTP server: `cluster time-service ntp server show`

```
cluster1::> cluster time-service ntp server show
Server          Version
-----
ntp1.example.com    auto
```

Related information

System administration

Commands for managing symmetric authentication on NTP servers

Beginning in ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this...	Use this command...
Configure an NTP server without symmetric authentication	<code>cluster time-service ntp server create -server server_name</code>
Configure an NTP server with symmetric authentication	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code>
Enable symmetric authentication for an existing NTP server An existing NTP server can be modified to enable authentication by adding the required key-id.	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>
Configure a shared NTP key	<code>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</code> Note: Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server
Configure an NTP server with an unknown key ID	<code>cluster time-service ntp server create -server server_name -key-id key_id</code>
Configure a server with a key ID not configured on the NTP server.	<code>cluster time-service ntp server create -server server_name -key-id key_id</code> Note: The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.
Disable symmetric authentication	<code>cluster time-service ntp server modify -server server_name -authentication disabled</code>

Decide where to send important event notifications

Before you configure important EMS event notifications, you need to decide whether to

send the notifications to an email address, a syslog server, or an SNMP traphost.

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

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

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

- Set EMS to send event notifications.

If you want...	Refer to this...
The EMS to send important event notifications to an email address	Configuring important EMS events to send email notifications
The EMS to forward important event notifications to a syslog server	Configuring important EMS events to forward notifications to a syslog server
If you want the EMS to forward event notifications to an SNMP traphost	Configuring SNMP traphosts to receive event notifications

Configure important EMS events to send email notifications

To receive email notifications for the most important events, you must configure the EMS to send email messages for events that signal important activity.

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

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

1. Configure the event SMTP mail server settings:

```
event config modify -mail-server mailhost.your_domain -mail-from  
cluster_admin@your_domain
```

2. Create an email destination for event notifications:

```
event notification destination create -name storage-admins -email  
your_email@your_domain
```

3. Configure the important events to send email notifications:

```
event notification create -filter-name important-events -destinations  
storage_admins
```

Configure important EMS events to forward notifications to a syslog server

To log notifications of the most severe events on a syslog server, you must configure the EMS to forward notifications for events that signal important activity.

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

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

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

1. Create a syslog server destination for important events:

```
event notification destination create -name syslog-ems -syslog syslog-server-address
```

2. Configure the important events to forward notifications to the syslog server:

```
event notification create -filter-name important-events -destinations syslog-ems
```

Configure SNMP traphosts to receive event notifications

To receive event notifications on an SNMP traphost, you must configure a traphost.

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



SNMP and SNMP traps are enabled by default.

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

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

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

1. If your environment does not already have an SNMP traphost configured to receive event notifications, add one: `system snmp traphost add -peer-address snmp_traphost_name`

All event notifications that are supported by SNMP by default are forwarded to the SNMP traphost.

Additional system configuration tasks to complete

After setting up a cluster, you can use either ONTAP System Manager or the ONTAP command-line interface (CLI) to continue configuring the cluster.

System configuration task	Resource
Configure networking: <ul style="list-style-type: none"> • Create broadcast domains • Create subnets • Create IP spaces 	Setting up the network
Set up the Service Processor	System administration
Lay out your aggregates	Disk and aggregate management
Create and configure data storage virtual machines (SVMs)	Cluster management using System Manager NFS configuration SMB/CIFS management SAN administration

Upgrade ONTAP

The [method you use to upgrade](#) your ONTAP software depends upon your configuration. If it is supported by your configuration, you should perform an automated nondisruptive upgrade (ANDU) using System Manager.

If you have an active [SupportEdge](#) contract for [Active IQ Digital Advisor](#), before you begin your upgrade, you should launch Upgrade Advisor in Active IQ Digital Advisor to help you plan your upgrade.

The content in this section will guide you through the steps you should take before and after you upgrade, including the resources you should read and the necessary pre- and post-upgrade checks you should perform.

What version of ONTAP can I upgrade to?

The version of ONTAP that you can upgrade to varies based on the version of ONTAP currently running on your nodes. You can determine the current version of ONTAP running on each node by using the `system image show` command.

You can upgrade from...	To...
ONTAP 9.9.0	ONTAP 9.9.1
ONTAP 9.8	ONTAP 9.9.0 or 9.9.1
ONTAP 9.7	ONTAP 9.8 or 9.9.1
ONTAP 9.6	ONTAP 9.7 or 9.8
ONTAP 9.5	ONTAP 9.6, 9.7, or 9.9.1 Note: If you are upgrading from ONTAP 9.5 directly to 9.9.1, you must download the software image for ONTAP 9.7 and 9.9.1. The automated upgrade process uses the 9.7 image in the background to complete the update to 9.9.1. You should expect multiple reboots during the process.
ONTAP 9.4	ONTAP 9.5
ONTAP 9.3	ONTAP 9.4, 9.5 or 9.7 Note: If you are upgrading from ONTAP 9.3 directly to 9.7, you must download the software image for ONTAP 9.5 and 9.7. The automated upgrade process uses the 9.5 image in the background to complete the update to 9.7. You should expect multiple reboots during the process.
ONTAP 9.2	ONTAP 9.3

You can upgrade from...	To...
ONTAP 9.1	ONTAP 9.2 or 9.3
ONTAP 9	ONTAP 9.1
Data ONTAP 8.3.x	ONTAP 9 or 9.1
Data ONTAP 8.2.x or earlier	Data ONTAP 8.3.x
Note: If you are running a release earlier than Data ONTAP 8.3.x, you cannot upgrade directly to ONTAP 9 or 9.1. You must upgrade to Data ONTAP 8.3.x first, then upgrade to ONTAP 9 or 9.1.	

How to plan your upgrade

You should use Upgrade Advisor, one of the services provided in NetApp [Active IQ](#) to plan your upgrade. Without Upgrade Advisor, you need to perform additional manual checks before upgrading.

Plan your upgrade with Upgrade Advisor

The Upgrade Advisor service in [Active IQ Digital Advisor](#) provides intelligence that helps you plan your upgrade and minimizes uncertainty and risk.

Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP. The Upgrade Advisor service helps you plan for a successful upgrade and provides a report of issues you might need to be aware of in the ONTAP version you're upgrading to.



An active SupportEdge contract is required for Active IQ.

1. [Launch Active IQ](#)
2. Review the Active IQ health summary to help assess the health of your cluster.
3. Review the recommended upgrade path and generate your upgrade plan.

Related information

[SupportEdge Services](#)

Plan your upgrade without Upgrade Advisor

It is a best practice to use Upgrade Advisor in [Active IQ](#) to plan your upgrade. If you do not have an active [SupportEdge](#) contract for Active IQ, you should perform the necessary pre-upgrade checks and create your own upgrade plan.

How long will my upgrade take?

You should plan for at least 30 minutes to complete preparatory steps, 60 minutes to upgrade each HA pair, and at least 30 minutes to complete post-upgrade steps.



If you are using NetApp Encryption with an external key management server and the Key Management Interoperability Protocol (KMIP), you should expect the upgrade for each HA pair to be longer than one hour.

Our upgrade duration guidelines are based on typical configurations and workloads. You can use these guidelines to estimate the time it will take to perform a nondisruptive upgrade in your environment. However, the actual duration of your upgrade process will depend on your individual environment and the number of nodes.

Resources to read before you upgrade

If you don't use [Active IQ Upgrade Advisor](#), you need to review a number of NetApp resources before upgrading your ONTAP software. These resources will help you understand issues you must resolve, new system behavior in the target release, and confirm hardware support.

1. Review the *Release Notes* for the target release.

[ONTAP 9 Release Notes](#)

The “Important cautions” section describes potential issues that you should be aware of before upgrading to the new release. The “New and changed features” and “Known problems and limitations” sections describe new system behavior after upgrading to the new release.

2. Confirm that your hardware platform is supported in the target release.

[NetApp Hardware Universe](#)

3. Confirm that your cluster and management switches are supported in the target release.

You can upgrade in a transitional state, but ultimately your NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions should be compatible with the version of ONTAP to which you are upgrading.

[NetApp Interoperability Matrix Tool](#)

4. If your cluster and management switches do not have the minimum software versions for the target ONTAP release, upgrade to supported software versions.

[NetApp Downloads: Cisco Ethernet Switch](#)

[NetApp Downloads: NetApp Ethernet Switch](#)

5. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.

All SAN components—including the target ONTAP software version, host OS and patches, required Host Utilities software, multipathing software, and adapter drivers and firmware—should be supported.

[NetApp Interoperability Matrix Tool](#)

6. If you are transitioning from 7-Mode using the 7-Mode Transition Tool, confirm that the tool supports transition to the ONTAP version to which you are upgrading.

All the projects in the tool must be in the completed or aborted state before you upgrade the 7-Mode Transition Tool that supports the ONTAP version to which you are upgrading.

[7-Mode Transition Tool installation and administration](#)

What to verify before upgrading

If you don't use [Active IQ Upgrade Advisor](#) to plan your upgrade, you should verify your cluster upgrade limits and your cluster activity before you upgrade.

Verify cluster upgrade limits

If you don't use [Active IQ Upgrade Advisor](#), you need to verify that your cluster does not exceed the platform system limits. SAN also has limits that you should verify in addition to the platform system limits.

1. Verify that the cluster does not exceed the system limits for your platform.

[NetApp Hardware Universe](#)

2. If your cluster is configured for SAN, verify that it does not exceed the configuration limits for FC, FCoE, and iSCSI.

[NetApp Hardware Universe](#)

3. Determine the CPU and disk utilization: `node run -node node_name -command sysstat -c 10 -x 3`

You should monitor CPU and disk utilization for 30 seconds. The values in the **CPU** and **Disk Util** columns should not exceed 50% for all 10 measurements reported. No additional load should be added to the cluster until the upgrade is complete.

NOTE: CPU and disk utilization can vary at different times in your environment. Therefore, it is best to check your CPU and disk utilization during the timeframe of your anticipated upgrade window.

Verify current cluster activity

If you don't use [Active IQ Upgrade Advisor](#), before upgrading, you should manually verify that no jobs are running and that any CIFS sessions that are not continuously available are terminated.

Verify that no jobs are running

Before upgrading the ONTAP software, you must verify the status of cluster jobs. If any aggregate, volume, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, you must allow the jobs to finish successfully or stop the queued entries.

1. Review the list of any running or queued aggregate, volume, or Snapshot jobs: `job show`

```

cluster1::> job show
          Owning
Job ID Name           Vserver   Node     State
-----
8629   Vol Reaper      cluster1   -        Queued
       Description: Vol Reaper Job
8630   Certificate Expiry Check
                           cluster1   -        Queued
       Description: Certificate Expiry Check
.
.
.

```

2. Delete any running or queued aggregate, volume, or Snapshot copy jobs: `job delete -id job_id`

```

cluster1::> job delete -id 8629

```

3. Verify that no aggregate, volume, or Snapshot jobs are running or queued: `job show`

In this example, all running and queued jobs have been deleted:

```

cluster1::> job show
          Owning
Job ID Name           Vserver   Node     State
-----
9944   SnapMirrorDaemon_7_2147484678
                           cluster1   node1     Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                           cluster1   node0     Dormant
       Description: SnapMirror Service Job
2 entries were displayed

```

Identifying active CIFS sessions that should be terminated

Before upgrading the ONTAP software, you should identify and gracefully terminate any CIFS sessions that are not continuously available.

Continuously available CIFS shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading.

1. Identify any established CIFS sessions that are not continuously available: `vserver cifs session show -continuously-available Yes -instance`

This command displays detailed information about any CIFS sessions that have no continuous availability.

You should terminate them before proceeding with the ONTAP upgrade.

```
cluster1::> vserver cifs session show -continuously-available Yes  
-instance  
  
          Node: node1  
          Vserver: vs1  
          Session ID: 1  
          Connection ID: 4160072788  
Incoming Data LIF IP Address: 198.51.100.5  
          Workstation IP address: 203.0.113.20  
          Authentication Mechanism: NTLMv2  
          Windows User: CIFSLAB\user1  
          UNIX User: nobody  
          Open Shares: 1  
          Open Files: 2  
          Open Other: 0  
          Connected Time: 8m 39s  
          Idle Time: 7m 45s  
          Protocol Version: SMB2_1  
Continuously Available: No  
1 entry was displayed.
```

2. If necessary, identify the files that are open for each CIFS session that you identified: `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1  
  
          Node:      node1  
          Vserver:    vs1  
          Connection: 4160072788  
          Session:    1  
          File      File      Open Hosting  
          Continuously  
          ID        Type      Mode Volume      Share           Available  
          -----  -----  -----  -----  
          -----  
          1        Regular   rw    vol10      homedirshare      No  
Path: \TestDocument.docx  
          2        Regular   rw    vol10      homedirshare      No  
Path: \file1.txt  
2 entries were displayed.
```

Related information

Considerations for session-oriented protocols

How firmware is updated during the ONTAP upgrade

Because upgrading ONTAP includes upgrading your firmware, you do not need to update firmware manually. When you perform an ONTAP upgrade, the firmware for your cluster included with the ONTAP upgrade package is copied to each node's boot device, and the new firmware is installed automatically.

Firmware for the following components is updated automatically if the version in your cluster is older than the firmware that is bundled with the ONTAP upgrade package:

- System and diagnostics:
 - BIOS
 - Flash Cache
 - Service Processor (SP)
- Disk
- Disk shelf

If desired, you can also update firmware manually in between ONTAP upgrades.

What to check before upgrading

Even if you use [Active IQ Upgrade Advisor](#) to plan your upgrade, there still are various pre-checks you should perform before you upgrade.

Verify cluster health

Before you upgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node          Health  Eligibility
-----
node0         true    true
node1         true    true
```

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Enter `y` to continue.
4. Verify the configuration details for each RDB process.

- The relational database epoch and database epochs should match for each node.
- The per-ring quorum master should be the same for all nodes.

Note that each ring might have a different quorum master.

To display this RDB process...	Enter this command...
Management application	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----  -----  -----  -----  -----  -----  -----
node0    vldb     154       154      14847   node0    master
node1    vldb     154       154      14847   node0    secondary
node2    vldb     154       154      14847   node0    secondary
node3    vldb     154       154      14847   node0    secondary
4 entries were displayed.
```

5. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -messagename scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```
cluster1::*> event log show -messagename scsiblade.*
Time          Node          Severity      Event
-----  -----
-----  -----
MM/DD/YYYY TIME  node0          INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1          INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
```

6. Return to the admin privilege level: `set -privilege admin`

Related information

[System administration](#)

Verify storage health

Before and after you upgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:

To check for...	Do this...
Broken disks	<ol style="list-style-type: none">Display any broken disks: <code>storage disk show -state broken</code>Remove or replace any broken disks.
Disks undergoing maintenance or reconstruction	<ol style="list-style-type: none">Display any disks in maintenance, pending, or reconstructing states: <code>'storage disk show -state maintenance</code>
pending	reconstructing' .. Wait for the maintenance or reconstruction operation to finish before proceeding. +

2. Verify that all aggregates are online by displaying the state: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you proceed with the upgrade.

Related information

[Logical storage management](#)

Verify SVM routing configuration

It is a best practice to configure one default route for an SVM. To avoid disruption, you should ensure that the default route is able to reach any network address that is not reachable by a more specific route. For more information, see [SU134: Network access might be disrupted by incorrect routing configuration in clustered ONTAP](#).

The routing table for an SVM determines the network path the SVM uses to communicate with a destination. It's important to understand how routing tables work so that you can prevent network problems before they occur.

Routing rules are as follows:

- ONTAP routes traffic over the most specific available route.
- ONTAP routes traffic over a default gateway route (having 0 bits of netmask) as a last resort, when more specific routes are not available.

In the case of routes with the same destination, netmask, and metric, there is no guarantee that the system will use the same route after a reboot or after an upgrade. This is especially an issue if you have configured multiple default routes.

Verifying the LIF failover configuration

Before you perform an upgrade, you must verify that the failover policies and failover groups are configured correctly.



During the upgrade process, LIFs are migrated based on the upgrade method. Depending upon the upgrade method, the LIF failover policy might or might not be used.

If you have 8 or more nodes in your cluster, the automated upgrade is performed using the batch method. The batch upgrade method involves dividing the cluster into multiple upgrade batches, upgrading the set of nodes in the first batch, upgrading their high-availability (HA) partners, and then repeating the process for the remaining batches. In ONTAP 9.7 and earlier, if the batch method is used, LIFs are migrated to the HA partner of the node being upgraded. In ONTAP 9.8 and later, if the batch method is used, LIFs are migrated to other batch group.

If you have less than 8 nodes in your cluster, the automated upgrade is performed using the rolling method. The rolling upgrade method involves initiating a failover operation on each node in an HA pair, updating the "failed" node, initiating giveback, and then repeating the process for each HA pair in the cluster. If the rolling method is used, LIFs are migrated to the failover target node as defined by the LIF failover policy.

1. Display the failover policy for each data LIF:

If your ONTAP version is...	Use this command
9.6 or later	<code>network interface show -service-policy data -failover</code>
9.5 or earlier	<code>network interface show -role data -failover</code>

This example shows the default failover configuration for a two-node cluster with two data LIFs:

```
cluster1::> network interface show -role data -failover
      Logical          Home          Failover          Failover
Vserver  Interface    Node:Port    Policy        Group
-----
-----
vs0
      lif0           node0:e0b    nextavail    system-
defined
      Failover Targets: node0:e0b, node0:e0c,
                         node0:e0d, node0:e0e,
                         node0:e0f, node1:e0b,
                         node1:e0c, node1:e0d,
                         node1:e0e, node1:e0f
vs1
      lif1           node1:e0b    nextavail    system-
defined
      Failover Targets: node1:e0b, node1:e0c,
                         node1:e0d, node1:e0e,
                         node1:e0f, node0:e0b,
                         node0:e0c, node0:e0d,
                         node0:e0e, node0:e0f
```

The **Failover Targets** field shows a prioritized list of failover targets for each LIF. For example, if lif0 fails over from its home port (e0b on node0), it's first attempts to fail over to port e0c on node0. If lif0 cannot fail over to e0c, it next attempts to fail over to port e0d on node0, and so on.

2. If the failover policy is set to disabled for any LIFs, other than SAN LIFs, use the `network interface modify` command to enable failover.
3. For each LIF, verify that the **Failover Targets** field includes data ports from a different node that will remain up while the LIF's home node is being upgraded.

You can use the `network interface failover-groups modify` command to add a failover target to the failover group.

Example

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vs1m-ucs572q:e0d,sti8-vs1m-ucs572r:e0d
```

Related information

[Network and LIF management](#)

Verify status

Before you upgrade, you should verify the following:

- HA pair status
- LDAP status (for ONTAP 9.2 or later)
- DNS server status (for ONTAP 9.2 or later),
- Networking and storage status (for MetroCluster configurations)

Verifying HA status

Before performing a nondisruptive upgrade, you should verify that storage failover is enabled for each HA pair. If the cluster consists of only two nodes, you should also verify that cluster HA is enabled.

You do not need to verify the HA status if you plan to perform a disruptive upgrade, because this upgrade method does not require storage failover.

1. Verify that storage failover is enabled and possible for each HA pair: `storage failover show`

This example shows that storage failover is enabled and possible on node0 and node1:

```
cluster1::> storage failover show
                           Takeover
  Node          Partner      Possible State
  -----        -----       -----
  -----
  node0        node1        true      Connected to node1
  node1        node0        true      Connected to node0
  2 entries were displayed.
```

If necessary, you can enable storage failover by using the `storage failover modify` command.

2. If the cluster consists of only two nodes (a single HA pair), verify that cluster HA is configured: `cluster ha show`

This example shows that cluster HA is configured:

```
cluster1::> cluster ha show
High Availability Configured: true
```

If necessary, you can enable cluster HA by using the `cluster ha modify` command.

Verifying LDAP status (ONTAP 9.2 and later)

Beginning in ONTAP 9.2, if LDAP is used by your storage virtual machines (SVMs), you must have an established LDAP connection to perform a nondisruptive upgrade. You should verify the LDAP connection before you begin the upgrade.

The task does not apply if you are upgrading from ONTAP 9.1 or earlier.

1. Check the LDAP status: `ldap check -vserver vserver_name`
2. If the LDAP status is down, modify it: `ldap client modify -client-config LDAP_client -ldap -servers ip_address`
3. Verify that the LDAP status is up: `ldap check -vserver vserver_name`

Verifying DNS server status (ONTAP 9.2 and later)

Beginning in ONTAP 9.2 and later, you should verify the status of your Domain Name Service (DNS) server before and after performing a nondisruptive upgrade.

The task does not apply if you are upgrading from ONTAP 9.1 or earlier.

1. Check the status of your DNS servers: `dns check -vserver vserver_name`

An up status indicates the service is running. A down status indicates that the service is not running.

2. If the DNS server is down, modify it: `dns modify -vserver vserver_name -domains domain_name -name-servers name_server_ipaddress`
3. Verify the status of the DNS server is up.

Verifying networking and storage status for MetroCluster configurations

Before and after performing an update in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status: `network interface show`

In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.

```

cluster1::> network interface show
      Logical      Status      Network          Current
Current Is
Vserver     Interface   Admin/Oper Address/Mask      Node      Port
Home
-----
-----
Cluster
      cluster1-a1_clus1
                  up/up    192.0.2.1/24      cluster1-01
                                                e2a
true
      cluster1-a1_clus2
                  up/up    192.0.2.2/24      cluster1-01
                                                e2b
true

cluster1-01
      clus_mgmt    up/up    198.51.100.1/24      cluster1-01
                                                e3a
true
      cluster1-a1_inet4_intercluster1
                  up/up    198.51.100.2/24      cluster1-01
                                                e3c
true
      ...
27 entries were displayed.

```

2. Verify the state of the aggregates: `storage aggregate show -state !online`

This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

This example shows a cluster in normal operation:

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State    #Vols  Nodes          RAID
Status
-----
-----
aggr0_b1
        0B       0B     0% offline      0 cluster2-01
raid_dp,
mirror

degraded
aggr0_b2
        0B       0B     0% offline      0 cluster2-02
raid_dp,
mirror

degraded
2 entries were displayed.
```

3. Verify the state of the volumes: `volume show -state !online`

This command displays any volumes that are *not* online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```

cluster1::> volume show -state !online
  (volume show)
Vserver    Volume      Aggregate   State     Type      Size
Available  Used%
-----  -----
vs2-mc    vol1        agg1_b1    -          RW       -
-
vs2-mc    root_vs2    agg0_b1    -          RW       -
-
vs2-mc    vol2        agg1_b1    -          RW       -
-
vs2-mc    vol3        agg1_b1    -          RW       -
-
vs2-mc    vol4        agg1_b1    -          RW       -
-
5 entries were displayed.

```

- Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you proceed with the upgrade.

Verify all LIFs are on home ports before upgrade

During a reboot, some LIFs might have been migrated to their assigned failover ports. Before and after you upgrade a cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

- Display the status of all LIFs: `network interface show`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```

cluster1::> network interface show -vserver vs0
      Logical      Status      Network          Current
Current Is
Vserver     Interface Admin/Oper Address/Mask      Node      Port
Home
-----
vs0
true       data001    down/down  192.0.2.120/24    node0    e0e
true       data002    down/down  192.0.2.121/24    node0    e0f
true       data003    down/down  192.0.2.122/24    node0    e2a
true       data004    down/down  192.0.2.123/24    node0    e2b
false      data005    down/down  192.0.2.124/24    node0    e0e
false      data006    down/down  192.0.2.125/24    node0    e0f
false      data007    down/down  192.0.2.126/24    node0    e2a
false      data008    down/down  192.0.2.127/24    node0    e2b
8 entries were displayed.

```

If any LIFs appear with a Status Admin status of down or with an Is home status of false, continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```

cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.

```

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

```

cluster1::> network interface revert *
8 entries were acted on.

```

4. Verify that all LIFs are in their home ports: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.

```

cluster1::> network interface show -vserver vs0
      Logical      Status      Network          Current
Current Is
Vserver       Interface Admin/Oper Address/Mask      Node      Port
Home
-----
vs0
true        data001    up/up     192.0.2.120/24    node0     e0e
true        data002    up/up     192.0.2.121/24    node0     e0f
true        data003    up/up     192.0.2.122/24    node0     e2a
true        data004    up/up     192.0.2.123/24    node0     e2b
true        data005    up/up     192.0.2.124/24    node1     e0e
true        data006    up/up     192.0.2.125/24    node1     e0f
true        data007    up/up     192.0.2.126/24    node1     e2a
true        data008    up/up     192.0.2.127/24    node1     e2b
8 entries were displayed.

```

Use Config Advisor to verify there are no common configuration errors

Before you upgrade, you can use the Config Advisor tool to check for common configuration errors.

Config Advisor is a configuration validation and health check tool for NetApp systems. This tool can be deployed at both secure sites and nonsecure sites for data collection and system analysis.



Support for Config Advisor is limited and is available only online.

1. Log in to the NetApp Support Site, and then navigate to **Downloads > Software > ToolChest**.
2. Click [Config Advisor](#).
3. Download, install, and run Config Advisor by following the directions on the web page.
4. After running Config Advisor, review the tool's output, and follow the recommendations that are provided to address any issues that are discovered by the tool.

Pre-upgrade checks

Depending on your environment, you need to consider certain factors before you start

your upgrade. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself...	If your answer is yes, then do this...
Do I have a mixed version cluster?	Check mixed version requirements
Do I have a SAN configuration?	Verify the SAN configuration
Do I have a MetroCluster configuration?	<ul style="list-style-type: none"> • Review specific upgrade requirements for MetroCluster configurations • Verify networking and storage status
Are nodes on my cluster using root-data partitioning and root-data-data-partitioning?	Examine upgrade considerations for root-data and root-data-data-partitioning
Do I have deduplicated volumes and aggregates?	Verify you have enough free space for your deduplicated volumes and aggregates
Is my cluster running SnapMirror?	<ul style="list-style-type: none"> • Review upgrade requirements for SnapMirror • Prepare your SnapMirror relationships for upgrade
Is my cluster running SnapLock?	Review upgrade considerations for SnapLock
Am I upgrading from ONTAP 8.3 and have load-sharing mirrors	Prepare all load-sharing mirrors for upgrade
Am I using NetApp Storage Encryption with external key management servers?	Delete any existing key management server connections
Do I have netgroups loaded into SVMs?	Verify that the netgroup file is present on each node
Do I have LDAP clients using SSLv3?	Configure LDAP clients to use TLS
Am I using session-oriented protocols?	Review considerations for session-oriented protocols

Mixed version requirements

Beginning with ONTAP 9.3, by default, you cannot join new nodes to the cluster that are running a version of ONTAP that is different from the version running on the existing nodes.

If you plan to add new nodes to your cluster that are running a version of ONTAP that is later than the nodes in your existing cluster, you should upgrade the nodes in your cluster to the later version first, then add the new nodes.

Mixed version clusters are not recommended, but in certain cases you might need to temporarily enter a mixed version state. For example, you need to enter a mixed version state if you are upgrading to a later version of ONTAP that is not supported on certain nodes in your existing cluster. In this case, you should upgrade the nodes that do support the later version of ONTAP, then unjoin the nodes that do not support the version of ONTAP you are upgrading to using the advance privilege `cluster unjoin -skip-lastlow-version -node check` command.

You might also need to enter a mixed version state for a technical refresh or an interrupted upgrade. In such

cases you can override the ONTAP 9.3 default behavior and join nodes of a different version using the following advance privilege commands:

- `cluster join -allow-mixed-version-join`
- `cluster add-node -allow-mixed-version-join`

When you have to enter a mixed version state, you should complete the upgrade as quickly as possible. An HA pair must not run an ONTAP version from a release that is different from other HA pairs in the cluster for more than seven days. For correct cluster operation, the period the cluster is in a mixed version state should be as short as possible.

When the cluster is in a mixed version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy the upgrade requirements.

Verifying the SAN configuration

Upgrading in a SAN environment changes which paths are direct. Therefore, before performing an upgrade, you should verify that each host is configured with the correct number of direct and indirect paths, and that each host is connected to the correct LIFs.

1. On each host, verify that a sufficient number of direct and indirect paths are configured, and that each path is active.

Each host must have a path to each node in the cluster.

2. Verify that each host is connected to a LIF on each node.

You should record the list of initiators for comparison after the upgrade.

For...	Enter...
iSCSI	<code>iscsi initiator show -fields igroup,initiator-name,tpgroup</code>
FC	<code>fcp initiator show -fields igroup,wwpn,lif</code>

MetroCluster configurations

Upgrade requirements for MetroCluster configurations

If you have to upgrade a MetroCluster configuration, you should be aware of some important requirements.

Required methods for performing major and minor upgrades of MetroCluster configurations

Patch upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure.

Starting with ONTAP 9.3, major upgrades to MetroCluster configurations can be performed with automatic non-disruptive upgrade (NDU) procedure. On systems running ONTAP 9.2 or earlier, major upgrades to

MetroCluster configurations must be performed with the NDU procedure that is specific to MetroCluster configurations.

General requirements

- Both clusters must be running the same version of ONTAP.

You can verify the ONTAP version by using the `version` command.

- The MetroCluster configuration must be in either normal or switchover mode.



Upgrade in switchover mode is only supported in minor patch upgrades.

- For all configurations except two-node clusters, you can nondisruptively upgrade both clusters at the same time.

For nondisruptive upgrade in two-node clusters, the clusters must be upgraded one node at a time.

- The aggregates in both clusters must not be in resyncing RAID status.

During MetroCluster healing, the mirrored aggregates are resynchronized. You can verify if the MetroCluster configuration is in this state by using the `storage aggregate plex show -in-progress true` command. If any aggregates are being synchronized, you should not perform an upgrade until the resynchronization is complete.

- Negotiated switchover operations will fail while the upgrade is in progress.

To avoid issues with upgrade or revert operations, do not attempt an unplanned switchover during an upgrade or revert operation unless all nodes on both clusters are running the same version of ONTAP.

Configuration requirements for normal operation

- The source SVM LIFs must be up and located on their home nodes.

Data LIFs for the destination SVMs are not required to be up or to be on their home nodes.

- All aggregates at the local site must be online.
- All root and data volumes owned by the local cluster's SVMs must be online.

Configuration requirements for switchover

- All LIFs must be up and located on their home nodes.
- All aggregates must be online, except for the root aggregates at the DR site.

Root aggregates at the DR site are offline during certain phases of switchover.

- All volumes must be online.

Related information

[Verifying networking and storage status for MetroCluster configurations](#)

Verify networking and storage status for MetroCluster configurations

Before performing an upgrade in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status: `network interface show`

In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.

```
cluster1::> network interface show
      Logical      Status      Network          Current
      Current Is
      Vserver      Interface   Admin/Oper Address/Mask      Node      Port
      Home
      -----
      -----
      Cluster
            cluster1-a1_clus1
                  up/up      192.0.2.1/24      cluster1-01
                                         e2a
      true
            cluster1-a1_clus2
                  up/up      192.0.2.2/24      cluster1-01
                                         e2b
      true

            cluster1-01
                  clus_mgmt    up/up      198.51.100.1/24      cluster1-01
                                         e3a
      true
            cluster1-a1_inet4_intercluster1
                  up/up      198.51.100.2/24      cluster1-01
                                         e3c
      true
            ...
      27 entries were displayed.
```

2. Verify the state of the aggregates: `storage aggregate show -state !online`

This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at the disaster recovery site are permitted to be offline.

This example shows a cluster in normal operation:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State    #Vols  Nodes          RAID
Status
-----
-----
aggr0_b1
        0B        0B    0% offline      0  cluster2-01
  raid_dp,
  mirror
  degraded
  aggr0_b2
        0B        0B    0% offline      0  cluster2-02
  raid_dp,
  mirror
  degraded
  2 entries were displayed.
```

3. Verify the state of the volumes: `volume show -state !online`

This command displays any volumes that are *not* online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```

cluster1::> volume show -state !online
  (volume show)
Vserver    Volume      Aggregate   State     Type      Size
Available  Used%
-----  -----
vs2-mc    vol1        agg1_b1    -          RW       -
-
vs2-mc    root_vs2    agg0_b1    -          RW       -
-
vs2-mc    vol2        agg1_b1    -          RW       -
-
vs2-mc    vol3        agg1_b1    -          RW       -
-
vs2-mc    vol4        agg1_b1    -          RW       -
-
5 entries were displayed.

```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you proceed with the upgrade.

Related information

[Upgrade requirements for MetroCluster configurations](#)

Upgrade considerations for root-data partitioning and root-data-data partitioning

Root-data partitioning and root-data-data-partitioning is supported for some platform models and configurations. This partitioning capability is enabled during system initialization; it cannot be applied to existing aggregates.

For information about migrating your data to a node that is configured for root-data partitioning or root-data-data partitioning, contact your account team or partner organization.

Related information

[ONTAP concepts](#)

Verify that deduplicated volumes and aggregates contain sufficient free space

Before upgrading ONTAP, you must verify that any deduplicated volumes and the aggregates that contain them have sufficient free space for the deduplication metadata. If there is insufficient free space, deduplication will be disabled when the ONTAP upgrade is completed.

Each deduplicated volume must contain at least 4% free space. Each aggregate that contains a deduplicated

volume must contain at least 3% free space.

1. Determine which volumes are deduplicated: `volume efficiency show`
2. Determine the free space available on each volume that you identified: `vol show -vserver Vserver_name -volume volume_name -fields volume, size, used, available, percent-used, junction-path`

Each deduplicated volume must not contain more than 96% used capacity. If necessary, you can increase the sizes of any volumes that exceed this capacity.

Logical storage management

In this example, the percent-used field displays the percentage of used space on the deduplicated volume.:

```
vserver      volume size      junction-path available used      percent-used
-----  -----  -----  -----
cluster1-01  vol0   22.99GB -                  14.11GB    7.73GB  35%
cluster1-02  vol0   22.99GB -                  12.97GB    8.87GB  40%
2 entries were displayed.
```

3. Identify the free space available on each aggregate that contains a deduplicated volume: `aggr show -aggregate aggregate_name -fields aggregate, size, usedsize, availsize, percent-used`

Each aggregate must not contain more than 97% used capacity. If necessary, you can increase the sizes of any aggregates that exceed this capacity.

Disk and aggregate management

In this example, the percent-used field displays the percentage of used space on the aggregate containing the deduplicated volume (aggr_2):

```
aggr show -aggregate aggregate_name -fields
aggregate, size, usedsize, availsize, percent-used
aggregate      availsize percent-used size      usedsize
-----  -----  -----
aggr0_cluster1_01  1.11GB    95%        24.30GB  23.19GB
aggr0_cluster1_02  1022MB    96%        24.30GB  23.30GB
2 entries were displayed.
```

SnapMirror

Upgrade requirements for SnapMirror

You must perform certain tasks to successfully upgrade a cluster that is running SnapMirror.

- If you are upgrading clusters with an inter-cluster DP SnapMirror relationship, you must upgrade the destination cluster before you upgrade the source cluster.
- Before upgrading a cluster that is running SnapMirror, SnapMirror operations must be quiesced for each node that contains destination volumes, and each peered SVM must have a unique name across the clusters.

For SnapMirror volume replication, the destination node must use an ONTAP version that is equal to or later than that of the SnapMirror source node. To prevent SnapMirror transfers from failing, you must suspend SnapMirror operations and, in some cases, upgrade destination nodes before upgrading source nodes. The following table describes the two options for suspending SnapMirror operations.

Option	Description	Upgrade destination nodes before source nodes?
Suspend SnapMirror operations for the duration of the NDU (nondisruptive upgrade).	The simplest method for upgrading in a SnapMirror environment is to suspend all SnapMirror operations, perform the upgrade, and then resume the SnapMirror operations. However, no SnapMirror transfers will occur during the entire NDU. You must use this method if your cluster contains nodes that are mirroring volumes to each other.	No, the nodes can be upgraded in any order.
Suspend SnapMirror operations one destination volume at a time.	You can suspend SnapMirror transfers for a particular destination volume, upgrade the node (or HA pair) that contains the destination volume, upgrade the node (or HA pair) that contains the source volume, and then resume the SnapMirror transfers for the destination volume. By using this method, SnapMirror transfers for all other destination volumes can continue while the nodes that contain the original destination and source volumes are upgraded.	Yes.

SVM peering requires SVM names to be unique across clusters. It is best practice to name SVMs with a unique fully qualified domain name (FQDN), for example, “dataVserver.HQ” or “mirrorVserver.Offsite”. Using the FQDN naming style makes it much easier to make sure of uniqueness.

Related information

[ONTAP concepts](#)

Prepare SnapMirror relationships for a nondisruptive upgrade

It is recommended that you quiesce your SnapMirror operations before performing a nondisruptive upgrade of ONTAP.

1. Use the snapmirror show command to determine the destination path for each SnapMirror relationship.
2. For each destination volume, suspend future SnapMirror transfers: `snapmirror quiesce -destination-path destination`

If there are no active transfers for the SnapMirror relationship, this command sets its status to Quiesced. If the relationship has active transfers, the status is set to Quiescing until the transfer is completed, and then the status becomes Quiesced.

This example quiesces transfers involving the destination volume vol1 from SVMvs0.example.com:

```
cluster1::> snapmirror quiesce -destination-path vs0.example.com:vol1
```

3. Verify that all SnapMirror relationships are quiesced: `snapmirror show -status !Quiesced`

This command displays any SnapMirror relationships that are *not* quiesced.

This example shows that all SnapMirror relationships are quiesced:

```
cluster1::> snapmirror show -status !Quiesced
There are no entries matching your query.
```

4. If any SnapMirror relationships are currently being transferred, do one of the following options:

Option	Description
Wait for the transfers to finish before performing the ONTAP upgrade.	After each transfer finishes, the relationship changes to Quiesced status.
Stop the transfers: <code>snapmirror abort -destination-path destination -h</code> Note: You must use the -foreground true parameter if you are aborting load-sharing mirror transfers.	This command stops the SnapMirror transfer and restores the destination volume to the last Snapshot copy that was successfully transferred. The relationship is set to Quiesced status.

Related information

[Upgrade requirements for SnapMirror](#)

[Upgrade considerations for SnapLock](#)

SnapLock does not allow the download of certain kernel versions if these are qualified as bad SnapLock releases or if SnapLock is disabled in those releases. These download restrictions only apply if the node has SnapLock data.

Prepare all load-sharing mirrors for a major upgrade

Before performing a major upgrade from ONTAP 8.3, you should move all of the load-sharing mirror source volumes to an aggregate on the node that you will upgrade last. This ensures that load-sharing mirror destination volumes are the same or later versions of ONTAP.

1. Record the locations of all load-sharing mirror source volumes.

Knowing where the load-sharing mirror source volumes came from helps facilitate returning them to their original locations after the major upgrade.

2. Determine the node and aggregate to which you will move the load-sharing mirror source volumes.
3. Move the load-sharing mirror source volumes to the node and aggregate by using the volume move start command.

Delete existing external key management server connections before upgrading

If you are using NetApp Storage Encryption (NSE) on ONTAP 9.2 or earlier and upgrading to ONTAP 9.3 or later, you must use the command line interface (CLI) to delete any existing external key management (KMIP) server connections before performing the upgrade.

1. Verify that the NSE drives are unlocked, open, and set to the default manufacture secure ID 0x0:
`storage encryption disk show -disk*`
2. Enter the advanced privilege mode:

`set -privilege advanced`
3. Use the default manufacture secure ID 0x0 to assign the FIPS key to the self-encrypting disks (SEDs):
`storage encryption disk modify -fips-key-id 0x0 -disk *`
4. Verify that assigning the FIPS key to all disks is complete:
`storage encryption disk show-status`
5. Verify that the **mode** for all disks is set to data:
`storage encryption disk show`
6. View the configured KMIP servers:
`security key-manager show`
7. Delete the configured KMIP servers:
`security key-manager delete -address kmip_ip_address`
8. Delete the external key manager configuration:
`security key-manager delete-kmip-config`



This step does not remove the NSE certificates.

After the upgrade is complete, you must reconfigure the KMIP server connections.

Related information

[Reconfiguring KMIP server connections after upgrading to ONTAP 9.3 or later](#)

Verifying that the netgroup file is present on all nodes

If you have loaded netgroups into storage virtual machines (SVMs), before you upgrade or revert, you must verify that the netgroup file is present on each node. A missing netgroup file on a node can cause an upgrade or revert to fail.

The *NFS Reference* contains more information about netgroups and loading them from a URI.

1. Set the privilege level to advanced: `set -privilege advanced`
2. Display the netgroup status for each SVM: `vserver services netgroup status`
3. Verify that for each SVM, each node shows the same netgroup file hash value: `vserver services name-service netgroup status`

If this is the case, you can skip the next step and proceed with the upgrade or revert. Otherwise, proceed to the next step.

4. On any one node of the cluster, manually load the netgroup file: `vserver services netgroup load -vserver vserver_name -source uri`

This command downloads the netgroup file on all nodes. If a netgroup file already exists on a node, it is overwritten.

Related information

[NFS management](#)

Configure LDAP clients to use TLS for highest security

Before upgrading to the target ONTAP release, you must configure LDAP clients using SSLv3 for secure communications with LDAP servers to use TLS. SSL will not be available after the upgrade.

By default, LDAP communications between client and server applications are not encrypted. You must disallow the use of SSL and enforce the use of TLS.

1. Verify that the LDAP servers in your environment support TLS.

If they do not, do not proceed. You should upgrade your LDAP servers to a version that supports TLS.

2. Check which ONTAP LDAP client configurations have LDAP over SSL/TLS enabled: `vserver services name-service ldap client show`

If there are none, you can skip the remaining steps. However, you should consider using LDAP over TLS for better security.

3. For each LDAP client configuration, disallow SSL to enforce the use of TLS: `vserver services name-service ldap client modify -vserver vserver_name -client-config ldap_client_config_name -allow-ssl false`
4. Verify that the use of SSL is no longer allowed for any LDAP clients: `vserver services name-service ldap client show`

Related information

NFS management

Considerations for session-oriented protocols

Clusters and session-oriented protocols might cause adverse effects on clients and applications in certain areas during upgrades.

If you are using session-oriented protocols, consider the following:

- CIFS

Hyper-V and SQL Server over SMB support nondisruptive operations (NDOs). If you configured a Hyper-V or SQL Server over SMB solution, the application servers and the contained virtual machines or databases remain online and provide continuous availability during the ONTAP upgrade.

For all other CIFS configurations, client sessions are terminated. You should direct users to end their sessions before you upgrade.

- NFSv4.x

NFSv4.x clients will automatically recover from connection losses experienced during the upgrade using normal NFSv4.x recovery procedures. Applications might experience a temporary I/O delay during this process.

- NDMP

State is lost and the client user must retry the operation.

- Backups and restores

State is lost and the client user must retry the operation.



Do not initiate a backup or restore during or immediately before an upgrade. Doing so might result in data loss.

- Applications (for example, Oracle or Exchange)

Effects depend on the applications. For timeout-based applications, you might be able to change the timeout setting to longer than the ONTAP reboot time to minimize adverse effects.

Download and install the ONTAP software image

You must first download the ONTAP software from the NetApp Support site; then you can install it.

Download the software image

For ONTAP 9.4 and later, you can copy the ONTAP software image from the NetApp Support Site to a local folder. For upgrades from ONTAP 9.3 or earlier, you must copy the ONTAP software image to an HTTP server or FTP server on your network.

You should note the following important information:

- Software images are specific to platform models.

You must obtain the correct image for your cluster. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site.

- Software images include the latest version of system firmware that was available when a given version of ONTAP was released.
- If you are upgrading a system with NetApp Volume Encryption to ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to upgrade a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

- If you are upgrading from ONTAP 9.5 to 9.9.1, you must copy the software image for ONTAP 9.7 and 9.9.1.
- If you are upgrading from ONTAP 9.3 to 9.7, you must copy the software image for ONTAP 9.5 and 9.7.

1. Locate the target ONTAP software in the [Software Downloads](#) area of the NetApp Support Site.

2. Copy the software image.

- For ONTAP 9.3 or earlier, copy the software image (for example, 93_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served.
- For ONTAP 9.4 or later, copy the software image (for example, 97_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served or to a local folder.

Install the software image

You must install the target software image on the cluster's nodes.

- If you are upgrading a system with NetApp Volume Encryption to ONTAP 9.5 or later, you must have downloaded the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to upgrade a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

- If you are upgrading from ONTAP 9.5 directly to 9.9.1, you must download the software image for ONTAP 9.7 and 9.9.1. If you are upgrading from ONTAP 9.3 directly to 9.7, you must download the software image for ONTAP 9.5 and 9.7.

The automated upgrade process uses both images in the background to complete the upgrade.

1. Set the privilege level to advanced, entering `y` when prompted to continue: `set -privilege advanced`

The advanced prompt (`*>`) appears.

For automatic nondisruptive upgrade (ANDU)

1. Check the image repository and delete any previous images.

```
cluster image package show-repository
```

```
cluster image package show-repository\  
<<smoke6-vsim-ucs6b4c#c-login_27|There are no packages in the  
repository.\r\n
```

2. Download the image.

```
cluster image package get -url url_to_image_on_nss
```

Example

```
cluster image package get -url http://10.60.132.98/x/eng/rlse/DOT/9.7P13X2/  
promo/9.7P13X2/x86_64.optimize/image.tgz
```

3. Verify the package is downloaded.

```
cluster image package show-repository
```

Example

```
cluster image package show-repository -fields download-ver\  
<<smoke6-vsim-ucs6b4c#c-login_27| download-verX;X\r\n  
<<smoke6-vsim-ucs6b4c#c-login_27| Downloaded VersionX;X\r\n<<smoke6-vsim-ucs6b4c#c-login_27| Stormking_9.10.0X;X\r\n
```

For manual upgrades

1. Download the image.

- If you are upgrading a non-MetroCluster configuration or a two-node MetroCluster configuration use the following command to download the image:

```
system node image update -node * -package location -replace-package true  
-setdefault true -background true
```



This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the -background parameter.

- If you are upgrading a four or eight-node MetroCluster configuration, you must issue the following command on both clusters:

```
system node image update -node * -package location -replace-package true  
-background true -setdefault false
```

This command uses an extended query to change the target software image, which is installed as the alternate image on each node.

2. Enter **y** to continue when prompted.

3. Verify that the software image is downloaded and installed on each node.

```
system node image show-update-progress -node *
```

This command displays the current status of the software image download and installation. You should continue to run this command until all nodes report a **Run Status** of **Exited**, and an **Exit Status** of **Success**.

The system node image update command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

This example shows a two-node cluster in which the software image is downloaded and installed successfully on both nodes:

```
cluster1:::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:          Run Script
    Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.

There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:          Run Script
    Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.

2 entries were acted on.
```

Which upgrade method should I use?

The method you use to upgrade depends upon your configuration. If available, the automated nondisruptive upgrade (ANDU) using System Manager is the preferred method.

- **Nondisruptive upgrade:** In a nondisruptive upgrade, update procedures are performed in the background while maintaining service to clients. Nondisruptive upgrades can be performed using an automated or manual method.
 - **Automated nondisruptive upgrade (ANDU)** can be executed using System Manager or the ONTAP command line interface (CLI). If available for your configuration, ANDU using System Manager is the recommended method of upgrade. With ANDU, ONTAP automatically installs the target ONTAP image on each node, validates the cluster components to ensure that the cluster can be upgraded nondisruptively, and then executes the upgrade in the background.
 - **Manual nondisruptive upgrade** involves manual steps to confirm the ONTAP configuration on each node and then uses the rolling update method to perform the upgrade. In the rolling update method, a

node is taken offline and upgraded while its partner takes over its storage. When the node upgrade is complete, the partner node gives control back to the original owning node and the process is repeated, this time on the partner node. Each additional HA pair is upgraded in sequence until all HA pairs are running the target release. Manual nondisruptive upgrades are executed using the ONTAP CLI.

- Disruptive:** In a disruptive upgrade, storage failover is disabled for each HA pair, and then each node is rebooted one at a time. Disruptive upgrades can be performed more quickly than nondisruptive upgrades, and require fewer steps to complete. However, you should not perform a disruptive upgrade unless you can take the cluster offline for the duration of the upgrade. If you are operating in a SAN environment, you should be prepared to shut down or suspend all SAN clients before performing a disruptive upgrade. Disruptive upgrades are performed using the ONTAP CLI.

You should only use a manual method if ANDU is not supported for your configuration.

Non-MCC configurations

The upgrade methods available for each configuration are listed in order of recommended usage.

ONTAP version	Number of nodes	Upgrade method
9.0 or later	2, 4, 8	<ul style="list-style-type: none"> Automated nondisruptive using System Manager Automated nondisruptive using the CLI Manual nondisruptive using the CLI (the Rolling Method) Manual disruptive using the CLI
9.0 or later	12	<ul style="list-style-type: none"> Automated nondisruptive using the CLI Manual nondisruptive using the CLI (the Rolling Method) Manual disruptive using the CLI
9.2 or later	Single-node	Automated disruptive using the CLI

MCC configurations

The upgrade methods available for each configuration are listed in order of recommended usage.

ONTAP version	Number of nodes	Upgrade method
9.3 or later	2,4	<ul style="list-style-type: none"> Automated nondisruptive using System Manager Automated nondisruptive using the CLI Manual disruptive using the CLI

ONTAP version	Number of nodes	Upgrade method
9.3 or later	8	<ul style="list-style-type: none"> • Automated nondisruptive using the CLI • Manual nondisruptive using the CLI • Manual disruptive using the CLI
9.2 or earlier	2	<ul style="list-style-type: none"> • Manual nondisruptive (for 2-node clusters) using the CLI • Manual disruptive using the CLI
9.2 or earlier	4, 8	<ul style="list-style-type: none"> • Manual nondisruptive using the CLI • Manual disruptive using the CLI
9.0 or later	4, 8 (patch only)	Automated nondisruptive using System Manager
9.2 or earlier	2, 4, 8 (patch only)	Automated nondisruptive using System Manager

Automated nondisruptive using System Manager

You can nondisruptively update the version of ONTAP on your cluster using System Manager.

Take a look at the simplified ONTAP upgrade capabilities available in ONTAP 9.8 System Manager.

ONTAP Upgrades Made Easy

Get the transformative features you've paid for!

Tech Clip

© 2020 NetApp, Inc. All rights reserved.



The update process checks your hardware platform and configuration to verify that your system is supported by the ONTAP version to which you are upgrading. ONTAP automatically shifts workloads during an upgrade between clusters so you can continue serving data.

This procedure updates your system to the specified version of ONTAP. It is assumed that your hardware platform and configuration is supported for the target release.



If issues are encountered during your automated upgrade, you can view EMS messages and details in ONTAP System Manager: Click **Events & Jobs > Events**.

Steps

1. If you want to download the software image to an HTTP or FTP server on your network, copy the software image from the NetApp support site to the directory on the HTTP or FTP server from which the image will be served.

If you want to download the software image to a local folder, then click the software image on the NetApp support site, select **Save As**, and then choose the local folder to place the image.

2. Depending on the System Manager version that you are running, perform one of the following steps:

ONTAP version	Steps
ONTAP 9.8 or later	Click Cluster > Overview .
ONTAP 9.5, or 9.6	Click Configuration > Cluster > Update .

ONTAP version	Steps
ONTAP 9.4 or earlier	Click Configuration > Cluster Update .

3. In the right corner of the Overview pane, click .
4. Click **ONTAP Update**.
5. In the Cluster Update tab, add a new image or select an available image.

If you want to...	Then...
Add a new software image from the local client Note: You should have already downloaded the image to the local client. Download and install the ONTAP software images	<ol style="list-style-type: none"> a. Under Available Software Images, click Add from Local. b. Browse to the location you saved the software image, select the image, and then click Open. The software image uploads after you click Open.
Add a new software image from the NetApp Support Site	<ol style="list-style-type: none"> a. Click Add from Server. b. In the Add a New Software Image dialog box, enter the URL of the HTTP server or FTP server on which you have saved the image that was downloaded from the NetApp Support Site. For anonymous FTP, you must specify the URL in the ftp://anonymous@ftpserver format. c. Click Add.
Select an available image	Choose one of the listed images.

6. Click **Validate** to run the pre-update validation checks to verify whether the cluster is ready for an update.

The validation operation checks the cluster components to validate that the update can be completed nondisruptively, and then displays any errors or warnings. It also displays any required remedial action that you must perform before updating the software.



You must perform all of the required remedial actions for the errors before proceeding with the update. Although you can ignore the remedial actions for the warnings, the best practice is to perform all of the remedial actions before proceeding with the update.

7. Click **Next**.
8. Click **Update**.

Validation is performed again.

- When the validation is complete, a table displays any errors and warnings, along with any required remedial actions to be taken before proceeding.

- If the validation is completed with warnings, you can choose to select the **Continue update with warnings** checkbox, and then click **Continue**.

When the validation is complete and the update is in progress, the update might be paused because of errors. You can click the error message to view the details, and then perform the remedial actions before resuming the update.

After the update is completed successfully, the node reboots, and you are redirected to the ONTAP System Manager login page. If the node takes a long time to reboot, you must refresh your browser.

Resuming an upgrade (using System Manager) after an error in the automated upgrade process

If an automated upgrade pauses because of an error, you can resolve the error and resume the automated upgrade, or you can cancel the automated upgrade and complete the process manually. If you choose to continue the automated upgrade, do not perform any of the upgrade steps manually.

1. Depending on the System Manager version that you are running, perform one of the following steps:
 - ONTAP 9.4 or earlier: Click **Configuration > Cluster Update**.
 - ONTAP 9.5 or 9.6: Click **Configuration > Cluster > Update**.
 - ONTAP 9.7 or later: Click **Cluster > Overview**

Then in the right corner of the Overview pane, click the three blue vertical dots, and **ONTAP Update**.

2. Continue the automated update or cancel it and continue manually.

If you want to...	Then...
Resume the automated updated	Click Resume .
Cancel the automated updated and continue manually	Click Cancel .

Automated nondisruptive using the CLI

You can use the command line interface (CLI) to verify that the cluster can be upgraded nondisruptively, install the target ONTAP image on each node, and then, execute an upgrade in the background.

If you do not plan to monitor the progress of the upgrade process, it is a good practice to [request EMS notifications of errors that might require manual intervention](#).

- You must have met the upgrade preparation requirements.
- For each HA pair, each node should have one or more ports on the same broadcast domain.

When a set of nodes is upgraded during a batch upgrade, the LIFs are migrated to the HA partner nodes. If the partners do not have any ports in the same broadcast domain, then the LIF migration fails.

- If you are upgrading from ONTAP 9.3 to 9.7, you must have obtained the software image for 9.5 and 9.7.

- If you are upgrading from ONTAP 9.5 to 9.9.1, you must have obtained the software image for 9.7 and 9.9.1.

The cluster image validate command checks the cluster components to validate that the upgrade can be completed nondisruptively, and then provides the status of each check and any required action you must take before performing the software upgrade.



Modifying the setting of the storage failover modify-auto-giveback command option before the start of an automatic nondisruptive upgrade (ANDU) has no impact on the upgrade process. The ANDU process ignores any preset value to this option during the takeover/giveback required for the update. For example, setting -autogiveback to false prior to beginning ANDU does not interrupt the automatic upgrade before giveback.

1. Delete the previous ONTAP software package:`cluster image package delete -version previous_ONTAP_Version`
2. Download the target ONTAP software package: `cluster image package get -url location`



If you are upgrading from ONTAP 9.3 to 9.7, download the software package for ONTAP 9.5, and then use the same command to download the software package for 9.7. If you are upgrading from ONTAP 9.5 to 9.9.1, download the software package for ONTAP 9.7, and then use the same command to download the software package for 9.9.1.

```
cluster1::> cluster image package get -url  
http://www.example.com/software/9.7/image.tgz
```

```
Package download completed.  
Package processing completed.
```

3. Verify that the software package is available in the cluster package repository: `cluster image package show-repository`

```
cluster1::> cluster image package show-repository  
Package Version  Package Build Time  
-----  -----  
9.7          MM/DD/YYYY 10:32:15
```

4. Verify that the cluster is ready to be upgraded nondisruptively: `cluster image validate -version package_version_number`

- If you are upgrading a two-node or four-node MetroCluster configuration, you must run this command on both clusters before proceeding.
- If you are upgrading from ONTAP 9.3 to 9.7, use the 9.7 package for verification. You do not need to validate the 9.5 package separately.
- If you are upgrading from ONTAP 9.5 to 9.9.1, use the 9.9.1 package for verification. You do not need to validate the 9.7 package separately.

```
cluster1::> cluster image validate -version 9.7
```

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed...

5. Monitor the progress of the validation: `cluster image show-update-progress`
6. Complete all required actions identified by the validation.
7. Generate a software upgrade estimate: `cluster image update -version package_version_number -estimate-only`

The software upgrade estimate displays details about each component to be updated, and the estimated duration of the upgrade.

8. Perform the software upgrade: `cluster image update -version package_version_number`
 - If you are upgrading from ONTAP 9.3 to 9.7, use the 9.7 package_version_number in the above command.
 - If you are upgrading from ONTAP 9.5 to 9.9.1, use the 9.9.1 package_version_number in the above command.
 - For any MetroCluster configuration, except a 2-node MetroCluster system, the upgrade process starts simultaneously on both of the clusters (the disaster recovery cluster and the production cluster) after the user provides a confirmation. For a 2-node MetroCluster system, the update is started first on the disaster recovery site, that is, the site where the upgrade is not initiated. After the update is fully completed on the disaster recovery site, the upgrade begins on the production site.
 - If the cluster consists of 2 through 6 nodes, a rolling upgrade is performed. If the cluster consists of 8 or more nodes, a batch upgrade is performed by default. If desired, you can use the `-force-rolling` parameter to specify a rolling upgrade instead.
 - After completing each takeover and giveback, the upgrade waits for 8 minutes to enable client applications to recover from the pause in I/O that occurs during the takeover and giveback. If your environment requires more or less time for client stabilization, you can use the `-stabilize-minutes` parameter to specify a different amount of stabilization time.

```

cluster1::> cluster image update -version 9.7

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status      Error-Action
-----
-----
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster1::>

```

9. Display the cluster update progress: `cluster image show-update-progress`



If you are upgrading a 4-node or 8-node MetroCluster configuration, the `cluster image show-update-progress` command only displays the progress for the node on which you run the command. You must run the command on each node to see individual node progress.

10. Verify that the upgrade was completed successfully on each node.

```

cluster1::> cluster image show-update-progress

                                         Estimated          Elapsed
Update Phase      Status           Duration        Duration
-----
Pre-update checks completed          00:10:00        00:02:07
Data ONTAP updates completed          01:31:00        01:39:00
Post-update checks completed          00:10:00        00:02:00
3 entries were displayed.

Updated nodes: node0, node1.

cluster1::>

```

11. Trigger an AutoSupport notification: `autosupport invoke -node * -type all -message "Finishing_NDU"`

If your cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

Related information

[Launch Active IQ](#)

[Active IQ documentation](#)

Resuming an upgrade (using the CLI) after an error in the automated upgrade process

If an automated upgrade pauses because of an error, you can resolve the error and resume the automated upgrade, or you can cancel the automated upgrade and complete the process manually. If you choose to continue the automated upgrade, do not perform any of the upgrade steps manually.

If you want to manually complete the upgrade, use the cluster image cancel-update command to cancel the automated process and proceed manually. If you want to continue the automated upgrade, complete the following steps.

1. View the upgrade error: `cluster image show-update-progress`
2. Resolve the error.
3. Resume the update: `cluster image resume-update`

Automated disruptive using the CLI (single-node cluster only)

Beginning with ONTAP 9.2, you can perform an automated update of a single-node cluster. Because single-node clusters lack redundancy, updates are always disruptive.

- You must have satisfied upgrade preparation requirements.
 1. Delete the previous ONTAP software package: `cluster image package delete -version previous_package_version`
 2. Download the target ONTAP software package: `cluster image package get -url location`

```
cluster1::> cluster image package get -url  
http://www.example.com/software/9.7/image.tgz  
  
Package download completed.  
Package processing completed.
```

3. Verify that the software package is available in the cluster package repository: `cluster image package show-repository`

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
-----
9.7            M/DD/YYYY 10:32:15
```

4. Verify that the cluster is ready to be upgraded: `cluster image validate -version package_version_number`

```
cluster1::> cluster image validate -version 9.7
```

WARNING: There are additional manual upgrade validation checks that must be performed after these automated validation checks have completed...

5. Monitor the progress of the validation: `cluster image show-update-progress`
6. Complete all required actions identified by the validation.
7. Optionally, generate a software upgrade estimate: `cluster image update -version package_version_number -estimate-only`

The software upgrade estimate displays details about each component to be updated, and the estimated duration of the upgrade.

8. Perform the software upgrade: `cluster image update -version package_version_number`



If an issue is encountered, the update pauses and prompts you to take corrective action. You can use the cluster image show-update-progress command to view details about any issues and the progress of the update. After correcting the issue, you can resume the update by using the cluster image resume-update command.

9. Display the cluster update progress: `cluster image show-update-progress`

The node is rebooted as part of the update and cannot be accessed while rebooting.

10. Trigger a notification: `autosupport invoke -node * -type all -message "Finishing_Upgrade"`

If your cluster is not configured to send messages, a copy of the notification is saved locally.

Manual nondisruptive using the CLI

Manual nondisruptive (rolling method) using the CLI

The rolling upgrade method enables you to update a cluster of two or more nodes nondisruptively. This method has several steps: initiating a failover operation on each node in an HA pair, updating the “failed” node, initiating giveback, and then repeating the process for each HA pair in the cluster.

You must have satisfied upgrade preparation requirements.

1. Update the first node in an HA pair

You upgrade the first node in an HA pair by initiating a takeover by the node's partner. The partner serves the node's data while the first node is upgraded.

2. Update the second node in an HA pair

After upgrading or downgrading the first node in an HA pair, you upgrade its partner by initiating a takeover on it. The first node serves the partner's data while the partner node is upgraded.

3. Repeat these steps for each additional HA pair.

You should complete post-upgrade tasks.

Updating the first node in an HA pair

You can update the first node in an HA pair by initiating a takeover by the node's partner. The partner serves the node's data while the first node is upgraded.

If you are performing a major upgrade, the first node to be upgraded must be the same node on which you configured the data LIFs for external connectivity and installed the first ONTAP image.

After upgrading the first node, you should upgrade the partner node as quickly as possible. Do not allow the two nodes to remain in a state of version mismatch longer than necessary.

1. Update the first node in the cluster by invoking an AutoSupport message: `autosupport invoke -node * -type all -message "Starting_NDU"`

This AutoSupport notification includes a record of the system status just prior to update. It saves useful troubleshooting information in case there is a problem with the update process.

If the cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

2. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

3. Set the new ONTAP software image to be the default image: `system image modify {-node nodenameA -iscurrent false} -isdefault true`

The system image modify command uses an extended query to change the new ONTAP software image (which is installed as the alternate image) to the default image for the node.

4. Monitor the progress of the update: `system node upgrade-revert show`

5. Verify that the new ONTAP software image is set as the default image: `system image show`

In the following example, image2 is the new ONTAP version and is set as the default image on node0:

```

cluster1::*> system image show
          Is      Is
          Node    Image  Default Current Version   Install
          -----  -----  -----  -----  -----
node0
          image1  false   true    X.X.X   MM/DD/YYYY TIME
          image2  true    false   Y.Y.Y   MM/DD/YYYY TIME
node1
          image1  true    true    X.X.X   MM/DD/YYYY TIME
          image2  false   false   Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

```

6. Disable automatic giveback on the partner node if it is enabled: `storage failover modify -node nodenameB -auto-giveback false`

If the cluster is a two-node cluster, a message is displayed warning you that disabling automatic giveback prevents the management cluster services from going online in the event of an alternating-failure scenario. Enter `y` to continue.

7. Verify that automatic giveback is disabled for node's partner: `storage failover show -node nodenameB -fields auto-giveback`

```

cluster1::> storage failover show -node node1 -fields auto-giveback
node      auto-giveback
-----
node1    false
1 entry was displayed.

```

8. Run the following command twice to determine whether the node to be updated is currently serving any clients `system node run -node nodenameA -command uptime`

The `uptime` command displays the total number of operations that the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, you must run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

NOTE: You should make a note of each protocol that has increasing client operations so that after the node is updated, you can verify that client traffic has resumed.

The following example shows a node with NFS, CIFS, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```

cluster1::> system node run -node node0 -command uptime
 2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
 2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops

```

9. Migrate all of the data LIFs away from the node: `network interface migrate-all -node nodenameA`
10. Verify any LIFs that you migrated: `network interface show`

For more information about parameters you can use to verify LIF status, see the `network interface show` man page.

The following example shows that node0's data LIFs migrated successfully. For each LIF, the fields included in this example enable you to verify the LIF's home node and port, the current node and port to which the LIF migrated, and the LIF's operational and administrative status.

```

cluster1::> network interface show -data-protocol nfs|cifs -role data
-hom-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
-----
vs0    data001 node0    e0a      node1    e0a      up       up
vs0    data002 node0    e0b      node1    e0b      up       up
vs0    data003 node0    e0b      node1    e0b      up       up
vs0    data004 node0    e0a      node1    e0a      up       up
4 entries were displayed.

```

11. Initiate a takeover: `storage failover takeover -ofnode nodenameA`

Do not specify the `-option immediate` parameter, because a normal takeover is required for the node that is being taken over to boot onto the new software image. If you did not manually migrate the LIFs away from the node, they automatically migrate to the node's HA partner to ensure that there are no service disruptions.

The first node boots up to the Waiting for giveback state.

NOTE: If AutoSupport is enabled, an AutoSupport message is sent indicating that the node is out of cluster quorum. You can ignore this notification and proceed with the update.

12. Verify that the takeover is successful: `storage failover show`

You might see error messages indicating version mismatch and mailbox format problems. This is expected

behavior and it represents a temporary state in a major nondisruptive upgrade and is not harmful.

The following example shows that the takeover was successful. Node node0 is in the Waiting for giveback state, and its partner is in the In takeover state.

```
cluster1::> storage failover show
               Takeover
Node          Partner      Possible State Description
-----  -----
-----  -----
node0          node1      -        Waiting for giveback (HA
mailboxes)
node1          node0      false    In takeover
2 entries were displayed.
```

13. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during takeover.

The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

14. Return the aggregates to the first node: `storage failover giveback -ofnode nodenameA`

The giveback first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates and any LIFs that were set to automatically revert. The newly booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

15. Verify that all aggregates have been returned: `storage failover show-giveback`

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

16. If any aggregates have not been returned, perform the following steps:

- a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
- [High-availability configuration](#)
- b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- c. Rerun the storage failover giveback command.

If you decided to override the “veto” condition, set the `-override-veto`s parameter to true.

17. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during giveback.

The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

18. Verify that the update was completed successfully for the node:

a. Go to the advanced privilege level :`set -privilege advanced`

b. Verify that update status is complete for the node: `system node upgrade-revert show -node nodenameA`

The status should be listed as complete.

If the status is not complete, from the node, run the system node upgrade-revert upgrade command. If the command does not complete the update, contact technical support.

c. Return to the admin privilege level: `set -privilege admin`

19. Verify that the node's ports are up: `network port show -node nodenameA`

You must run this command on a node that is upgraded to the higher version of ONTAP 9.

The following example shows that all of the node's ports are up:

```
cluster1::> network port show -node node0
                                         Speed
(Mbps)
Node    Port      IPspace      Broadcast Domain Link     MTU     Admin/Oper
-----  -----  -----
-----  -----
node0
    e0M      Default      -
                up        1500   auto/100
    e0a      Default      -
                up        1500   auto/1000
    e0b      Default      -
                up        1500   auto/1000
    e1a      Cluster      Cluster
                up        9000   auto/10000
    e1b      Cluster      Cluster
                up        9000   auto/10000
5 entries were displayed.
```

20. Revert the LIFs back to the node: `network interface revert *`

This command returns the LIFs that were migrated away from the node.

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. Verify that the node's data LIFs successfully reverted back to the node, and that they are up: `network interface show`

The following example shows that all of the data LIFs hosted by the node have successfully reverted back to the node, and that their operational status is up:

```

cluster1::> network interface show
      Logical      Status      Network          Current
Current Is
Vserver       Interface Admin/Oper Address/Mask      Node      Port
Home
-----
vs0
true          data001    up/up     192.0.2.120/24    node0    e0a
true          data002    up/up     192.0.2.121/24    node0    e0b
true          data003    up/up     192.0.2.122/24    node0    e0b
true          data004    up/up     192.0.2.123/24    node0    e0a
4 entries were displayed.

```

22. If you previously determined that this node serves clients, verify that the node is providing service for each protocol that it was previously serving: `system node run -node nodenameA -command uptime`

The operation counts reset to zero during the update.

The following example shows that the updated node has resumed serving its NFS and iSCSI clients:

```

cluster1::> system node run -node node0 -command uptime
 3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops

```

23. Reenable automatic giveback on the partner node if it was previously disabled: `storage failover modify -node nodenameB -auto-giveback true`

You should proceed to update the node's HA partner as quickly as possible. If you must suspend the update process for any reason, both nodes in the HA pair should be running the same ONTAP version.

Updating the partner node in an HA pair

After updating the first node in an HA pair, you update its partner by initiating a takeover on it. The first node serves the partner's data while the partner node is upgraded.

1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

2. Set the new ONTAP software image to be the default image: `system image modify {-node nodenameB -iscurrent false} -isdefault true`

The system image modify command uses an extended query to change the new ONTAP software image (which is installed as the alternate image) to be the default image for the node.

3. Monitor the progress of the update: `system node upgrade-revert show`
4. Verify that the new ONTAP software image is set as the default image: `system image show`

In the following example, `image2` is the new version of ONTAP and is set as the default image on the node:

```
cluster1::*> system image show
      Is      Is          Install
      Node    Image  Default Current Version     Date
-----  -----  -----  -----  -----
node0
      image1  false   false   X.X.X   MM/DD/YYYY TIME
      image2  true    true    Y.Y.Y   MM/DD/YYYY TIME
node1
      image1  false   true    X.X.X   MM/DD/YYYY TIME
      image2  true    false   Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.
```

5. Disable automatic giveback on the partner node if it is enabled: `storage failover modify -node nodenameA -auto-giveback false`

If the cluster is a two-node cluster, a message is displayed warning you that disabling automatic giveback prevents the management cluster services from going online in the event of an alternating-failure scenario. Enter `y` to continue.

6. Verify that automatic giveback is disabled for the partner node: `storage failover show -node nodenameA -fields auto-giveback`

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node      auto-giveback
-----
node0    false
1 entry was displayed.
```

7. Run the following command twice to determine whether the node to be updated is currently serving any clients: `system node run -node nodenameB -command uptime`

The uptime command displays the total number of operations that the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, you must run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

NOTE: You should make a note of each protocol that has increasing client operations so that after the node

is updated, you can verify that client traffic has resumed.

The following example shows a node with NFS, CIFS, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster1::> system node run -node node1 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Migrate all of the data LIFs away from the node: `network interface migrate-all -node nodenameB`
9. Verify the status of any LIFs that you migrated: `network interface show`

For more information about parameters you can use to verify LIF status, see the `network interface show` man page.

The following example shows that node1's data LIFs migrated successfully. For each LIF, the fields included in this example enable you to verify the LIF's home node and port, the current node and port to which the LIF migrated, and the LIF's operational and administrative status.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif      home-node home-port curr-node curr-port status-oper
status-admin
-----
-----
vs0    data001 node1    e0a        node0    e0a        up       up
vs0    data002 node1    e0b        node0    e0b        up       up
vs0    data003 node1    e0b        node0    e0b        up       up
vs0    data004 node1    e0a        node0    e0a        up       up
4 entries were displayed.
```

10. Initiate a takeover: `storage failover takeover -ofnode nodenameB -option allow-version-mismatch`

Do not specify the `-option immediate` parameter, because a normal takeover is required for the node that is being taken over to boot onto the new software image. If you did not manually migrate the LIFs away from the node, they automatically migrate to the node's HA partner so that there are no service disruptions.

The node that is taken over boots up to the Waiting for giveback state.

NOTE: If AutoSupport is enabled, an AutoSupport message is sent indicating that the node is out of cluster

quorum. You can ignore this notification and proceed with the update.

11. Verify that the takeover was successful: `storage failover show`

The following example shows that the takeover was successful. Node node1 is in the Waiting for giveback state, and its partner is in the In takeover state.

```
cluster1::> storage failover show
                           Takeover
      Node          Partner      Possible State Description
-----  -----  -----
-----  -----
node0        node1          -       In takeover
node1        node0          false   Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

12. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in I/O that occurs during takeover.

The recovery time is client-specific and might take longer than eight minutes, depending on the characteristics of the client applications.

13. Return the aggregates to the partner node: `storage failover giveback -ofnode nodenameB`

The giveback operation first returns the root aggregate to the partner node and then, after that node has finished booting, returns the non-root aggregates and any LIFs that were set to automatically revert. The newly booted node begins to serve data to clients from each aggregate as soon as the aggregate is returned.

14. Verify that all aggregates are returned: `storage failover show-giveback`

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates are returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback operation.

15. If any aggregates are not returned, perform the following steps:

- a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.

[High-availability configuration](#)

- b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- c. Rerun the storage failover giveback command.

If you decided to override the “veto” condition, set the `-override-veto`s parameter to true.

16. Wait at least eight minutes for the following conditions to take effect:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in an I/O operation that occurs during giveback.

The recovery time is client specific and might take longer than eight minutes, depending on the characteristics of the client applications.

17. Verify that the update was completed successfully for the node:

- Go to the advanced privilege level : `set -privilege advanced`
- Verify that update status is complete for the node: `system node upgrade-revert show -node nodenameB`

The status should be listed as complete.

If the status is not complete, from the node, run the `system node upgrade-revert upgrade` command. If the command does not complete the update, contact technical support.

- Return to the admin privilege level: `set -privilege admin`

18. Verify that the node's ports are up: `network port show -node nodenameB`

You must run this command on a node that has been upgraded to ONTAP 9.4.

The following example shows that all of the node's data ports are up:

```
cluster1::> network port show -node node1
                                         Speed
                                         (Mbps)
Node    Port      IPspace      Broadcast Domain Link     MTU     Admin/Oper
-----  -----  -----
-----  -----
node1
      e0M      Default      -
                  up        1500  auto/100
      e0a      Default      -
                  up        1500  auto/1000
      e0b      Default      -
                  up        1500  auto/1000
      e1a      Cluster      Cluster
                  up        9000  auto/10000
      e1b      Cluster      Cluster
                  up        9000  auto/10000
5 entries were displayed.
```

19. Revert the LIFs back to the node: `network interface revert *`

This command returns the LIFs that were migrated away from the node.

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. Verify that the node's data LIFs successfully reverted back to the node, and that they are up: `network interface show`

The following example shows that all of the data LIFs hosted by the node is successfully reverted back to the node, and that their operational status is up:

```
cluster1::> network interface show
      Logical      Status      Network          Current
      Current Is
Vserver     Interface  Admin/Oper Address/Mask      Node      Port
Home
-----
----- vs0
true        data001    up/up     192.0.2.120/24    node1     e0a
true        data002    up/up     192.0.2.121/24    node1     e0b
true        data003    up/up     192.0.2.122/24    node1     e0b
true        data004    up/up     192.0.2.123/24    node1     e0a
4 entries were displayed.
```

21. If you previously determined that this node serves clients, verify that the node is providing service for each protocol that it was previously serving: `system node run -node nodenameB -command uptime`

The operation counts reset to zero during the update.

The following example shows that the updated node has resumed serving its NFS and iSCSI clients:

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. If this was the last node in the cluster to be updated, trigger an AutoSupport notification: `autosupport invoke -node * -type all -message "Finishing_NDU"`

This AutoSupport notification includes a record of the system status just prior to update. It saves useful troubleshooting information in case there is a problem with the update process.

If the cluster is not configured to send AutoSupport messages, a copy of the notification is saved locally.

23. Confirm that the new ONTAP software is running on both nodes of the HA pair: `system node image show`

In the following example, image2 is the updated version of ONTAP and is the default version on both nodes:

```

cluster1::*> system node image show
          Is      Is           Install
          Node    Image  Default Current Version   Date
-----
node0
          image1  false  false   X.X.X  MM/DD/YYYY TIME
          image2  true   true   Y.Y.Y  MM/DD/YYYY TIME
node1
          image1  false  false   X.X.X  MM/DD/YYYY TIME
          image2  true   true   Y.Y.Y  MM/DD/YYYY TIME
4 entries were displayed.

```

24. Reenable automatic giveback on the partner node if it was previously disabled: `storage failover modify -node nodenameA -auto-giveback true`
25. Verify that the cluster is in quorum and that services are running by using the cluster show and cluster ring show (advanced privilege level) commands.

You must perform this step before upgrading any additional HA pairs.

26. Return to the admin privilege level: `set -privilege admin`

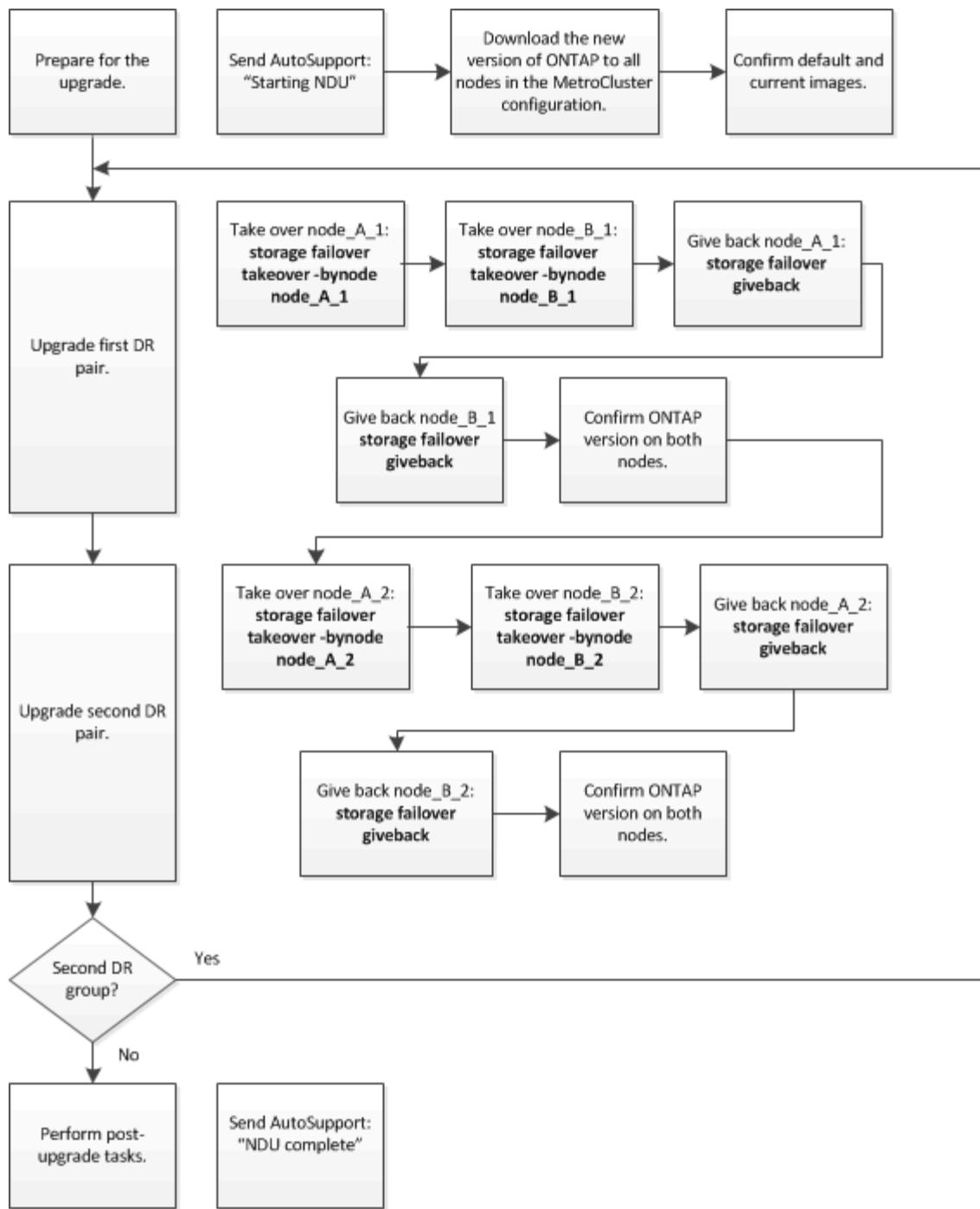
Upgrade any additional HA pairs.

MCC configurations

Manual nondisruptive upgrade of a four- or eight-node MetroCluster configuration using the CLI

The manual update procedure for upgrading or downgrading a four- or eight-node MetroCluster configuration involves preparing for the update, updating the DR pairs in each of the one or two DR groups simultaneously, and performing some post-update tasks.

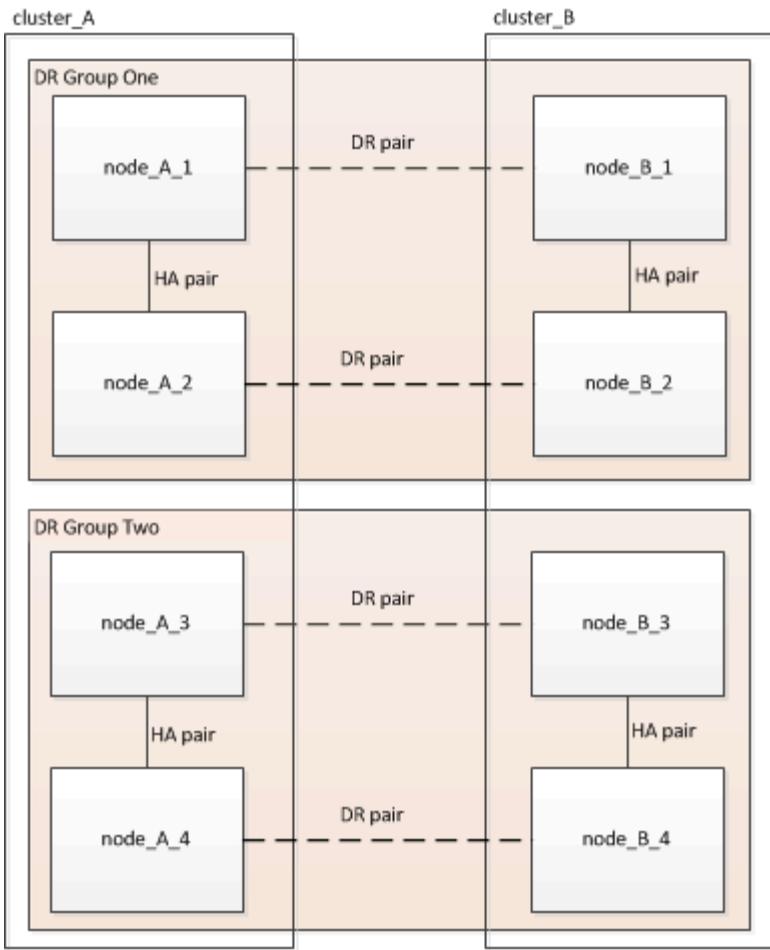
- This task applies to the following configurations:
 - Four-node MetroCluster FC or IP configurations running ONTAP 9.2 or earlier
 - Eight-node MetroCluster FC configurations, regardless of ONTAP version
- If you have a two-node MetroCluster configuration, do not use this procedure.
- The following tasks refer to the old and new versions of ONTAP.
 - When upgrading, the old version is a previous version of ONTAP, with a lower version number than the new version of ONTAP.
 - When downgrading, the old version is a later version of ONTAP, with a higher version number than the new version of ONTAP.
- This task uses the following high-level workflow:



Differences when updating software on an eight-node or four-node MetroCluster configuration

The MetroCluster software update process differs, depending on whether there are eight or four nodes in the MetroCluster configuration.

A MetroCluster configuration consists of one or two DR groups. Each DR group consists of two HA pairs, one HA pair at each MetroCluster cluster. An eight-node MetroCluster includes two DR groups:



The MetroCluster software update procedure involves upgrading or downgrading one DR group at a time.

For four-node MetroCluster configurations:

1. Update DR Group One:
 - a. Update node_A_1 and node_B_1.
 - b. Update node_A_2 and node_B_2.

For eight-node MetroCluster configurations, you perform the DR group update procedure twice:

1. Update DR Group One:
 - a. Update node_A_1 and node_B_1.
 - b. Update node_A_2 and node_B_2.
2. Update DR Group Two:
 - a. Update node_A_3 and node_B_3.
 - b. Update node_A_4 and node_B_4.

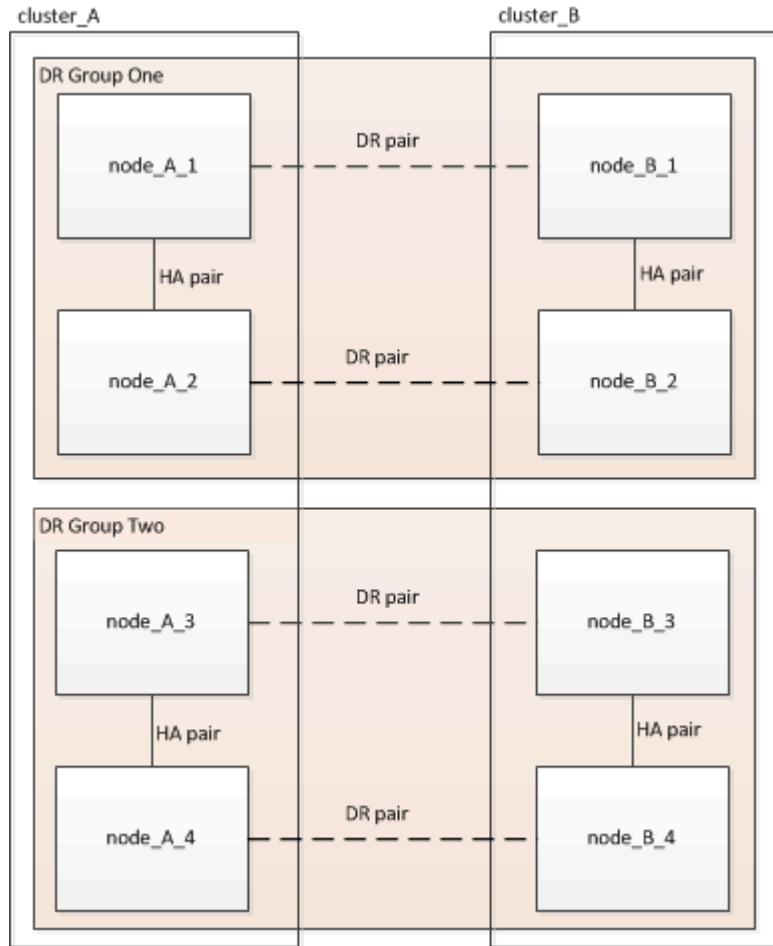
Preparing to update a MetroCluster DR group

Before you actually update the software on the nodes, you must identify the DR relationships among the nodes, send an AutoSupport message that you are initiating an update, and confirm the ONTAP version running on each node.

You must have [downloaded and installed the software images](#).

This task must be repeated on each DR group. If the MetroCluster configuration consists of eight nodes, there are two DR groups. Thereby, this task must be repeated on each DR group.

The examples provided in this task use the names shown in the following illustration to identify the clusters and nodes:



1. Identify the DR pairs in the configuration: `metrocluster node show -fields dr-partner`

```
cluster_A::> metrocluster node show -fields dr-partner
(metrocluster node show)
dr-group-id cluster      node      dr-partner
-----  -----
1        cluster_A    node_A_1    node_B_1
1        cluster_A    node_A_2    node_B_2
1        cluster_B    node_B_1    node_A_1
1        cluster_B    node_B_2    node_A_2
4 entries were displayed.
```

```
cluster_A::>
```

2. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

3. Confirm the ONTAP version running on each node:

- a. Confirm the version on cluster_A: `system image show`

```
cluster_A::*> system image show
      Is      Is
      Node    Image  Default Current Version   Install
      -----  -----  -----  -----
node_A_1
      image1  true   true   X.X.X   MM/DD/YYYY TIME
      image2  false  false  Y.Y.Y   MM/DD/YYYY TIME
node_A_2
      image1  true   true   X.X.X   MM/DD/YYYY TIME
      image2  false  false  Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.
```

```
cluster_A::>
```

- b. Confirm the version on cluster_B: `system image show`

```
cluster_B::*> system image show
      Is      Is
      Node    Image  Default Current Version   Install
      -----  -----  -----  -----
node_B_1
      image1  true   true   X.X.X   MM/DD/YYYY TIME
      image2  false  false  Y.Y.Y   MM/DD/YYYY TIME
node_B_2
      image1  true   true   X.X.X   MM/DD/YYYY TIME
      image2  false  false  Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.
```

```
cluster_B::>
```

4. Trigger an AutoSupport notification: `autosupport invoke -node * -type all -message "Starting_NDU"`

This AutoSupport notification includes a record of the system status before the update. It saves useful troubleshooting information if there is a problem with the update process.

If your cluster is not configured to send AutoSupport messages, then a copy of the notification is saved locally.

5. For each node in the first set, set the target ONTAP software image to be the default image: `system image modify {-node nodename -iscurrent false} -isdefault true`

This command uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

6. Verify that the target ONTAP software image is set as the default image:

- a. Verify the images on cluster_A: `system image show`

In the following example, image2 is the new ONTAP version and is set as the default image on each of the nodes in the first set:

```
cluster_A::*> system image show
      Is      Is          Install
      Node    Image  Default Current Version Date
-----
node_A_1
      image1  false   true     X.X.X  MM/DD/YYYY TIME
      image2  true    false    Y.Y.Y  MM/DD/YYYY TIME
node_A_2
      image1  false   true     X.X.X  MM/DD/YYYY TIME
      image2  true    false    Y.Y.Y  MM/DD/YYYY TIME

2 entries were displayed.
```

- b. Verify the images on cluster_B: `system image show`

The following example shows that the target version is set as the default image on each of the nodes in the first set:

```
cluster_B::*> system image show
      Is      Is          Install
      Node    Image  Default Current Version Date
-----
node_A_1
      image1  false   true     X.X.X  MM/DD/YYYY TIME
      image2  true    false    Y.Y.Y  MM/YY/YYYY TIME
node_A_2
      image1  false   true     X.X.X  MM/DD/YYYY TIME
      image2  true    false    Y.Y.Y  MM/DD/YYYY TIME

2 entries were displayed.
```

7. Determine whether the nodes to be upgraded are currently serving any clients by entering the following command twice for each node: `system node run -node target-node -command uptime`

The uptime command displays the total number of operations that the node has performed for NFS, CIFS, FC, and iSCSI clients since the node was last booted. For each protocol, you need to run the command twice to determine whether the operation counts are increasing. If they are increasing, the node is currently serving clients for that protocol. If they are not increasing, the node is not currently serving clients for that protocol.

NOTE: You should make a note of each protocol that has increasing client operations so that after the node is upgraded, you can verify that client traffic has resumed.

This example shows a node with NFS, CIFS, FC, and iSCSI operations. However, the node is currently serving only NFS and iSCSI clients.

```
cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster_x::> system node run -node node0 -command uptime
2:58pm up 7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

Updating the first DR pair in a MetroCluster DR group

You must perform a takeover and giveback of the nodes in the correct order to make the new version of ONTAP the current version of the node.

All nodes must be running the old version of ONTAP.

In this task, node_A_1 and node_B_1 are updated.

If you have updated the ONTAP software on the first DR group, and are now updating the second DR group in an eight-node MetroCluster configuration, in this task you would be updating node_A_3 and node_B_3.

1. If MetroCluster Tiebreaker software is enabled, disable it.
2. For each node in the HA pair, disable automatic giveback: `storage failover modify -node target-node -auto-giveback false`

This command must be repeated for each node in the HA pair.

3. Verify that automatic giveback is disabled: `storage failover show -fields auto-giveback`

This example shows that automatic giveback has been disabled on both nodes:

```
cluster_x::> storage failover show -fields auto-giveback
node      auto-giveback
-----
node_x_1  false
node_x_2  false
2 entries were displayed.
```

4. Ensure that I/O is not exceeding ~50% for each controller. Ensure that CPU utilization is not exceeding ~50% per controller.

5. Initiate a takeover of the target node on cluster_A:

Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

a. Take over the DR partner on cluster_A (node_A_1):
`storage failover takeover -ofnode node_A_1`

The node boots up to the "Waiting for giveback" state.



If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

b. Verify that the takeover is successful: `storage failover show`

The following example shows that the takeover is successful. Node_A_1 is in the "Waiting for giveback" state and node_A_2 is in the "In takeover" state.

```
cluster1::> storage failover show
                           Takeover
      Node          Partner      Possible State Description
      -----        -----       -----
      -----
      node_A_1      node_A_2      -           Waiting for giveback (HA
      mailboxes)
      node_A_2      node_A_1      false        In takeover
      2 entries were displayed.
```

6. Take over the DR partner on cluster_B (node_B_1):

Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

a. Take over node_B_1: `storage failover takeover -ofnode node_B_1`

The node boots up to the "Waiting for giveback" state.



If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

b. Verify that the takeover is successful: `storage failover show`

The following example shows that the takeover is successful. Node_B_1 is in the "Waiting for giveback" state and node_B_2 is in the "In takeover" state.

```

cluster1::> storage failover show
                           Takeover
      Node          Partner      Possible State Description
      -----
      -----
      node_B_1      node_B_2      -        Waiting for giveback (HA
      mailboxes)
      node_B_2      node_B_1      false    In takeover
      2 entries were displayed.

```

7. Wait at least eight minutes to ensure the following conditions:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in I/O that occurs during takeover.

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

8. Return the aggregates to the target nodes:

After upgrading MetroCluster IP configurations to ONTAP 9.5 or later, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

- a. Give back the aggregates to the DR partner on cluster_A: `storage failover giveback -ofnode node_A_1`
- b. Give back the aggregates to the DR partner on cluster_B: `storage failover giveback -ofnode node_B_1`

The giveback operation first returns the root aggregate to the node and then, after the node has finished booting, returns the non-root aggregates.

9. Verify that all aggregates have been returned by issuing the following command on both clusters: `storage failover show-giveback`

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

10. If any aggregates have not been returned, do the following:

- a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
- b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- c. Reenter the storage failover giveback command.

If you decided to override the “veto” condition, set the `-override-veto`s parameter to true.

11. Wait at least eight minutes to ensure the following conditions:

- Client multipathing (if deployed) is stabilized.

- Clients are recovered from the pause in I/O that occurs during giveback.

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

- Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

- Confirm the version on cluster_A: `system image show`

The following example shows that System image2 should be the default and current version on node_A_1:

```
cluster_A::*> system image show
      Is      Is          Install
Node    Image  Default Current Version Date
-----
node_A_1
      image1  false   false     X.X.X  MM/DD/YYYY TIME
      image2  true    true     Y.Y.Y  MM/DD/YYYY TIME
node_A_2
      image1  false   true     X.X.X  MM/DD/YYYY TIME
      image2  true    false    Y.Y.Y  MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

- Confirm the version on cluster_B: `system image show`

The following example shows that System image2 (ONTAP 9.0.0) is the default and current version on node_A_1:

```
cluster_A::*> system image show
      Is      Is          Install
Node    Image  Default Current Version Date
-----
node_B_1
      image1  false   false     X.X.X  MM/DD/YYYY TIME
      image2  true    true     Y.Y.Y  MM/DD/YYYY TIME
node_B_2
      image1  false   true     X.X.X  MM/DD/YYYY TIME
      image2  true    false    Y.Y.Y  MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

Updating the second DR pair in a MetroCluster DR group

You must perform a takeover and giveback of the node in the correct order to make the new version of ONTAP the current version of the node.

You should have upgraded the first DR pair (node_A_1 and node_B_1).

In this task, node_A_2 and node_B_2 are updated.

If you have updated the ONTAP software on the first DR group, and are now updating the second DR group in an eight-node MetroCluster configuration, in this task you are updating node_A_4 and node_B_4.

1. Initiate a takeover of the target node on cluster_A:

Do not specify the -option immediate parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

- a. Take over the DR partner on cluster_A:

If you are upgrading from ...	Enter this command...
ONTAP 9.1	<code>storage failover takeover -ofnode node_A_2</code>
ONTAP 9.0 or Data ONTAP 8.3.x	<code>storage failover takeover -ofnode node_A_2 -option allow-version-mismatch</code> The <code>allow-version-mismatch</code> option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.

The node boots up to the "Waiting for giveback" state.



If AutoSupport is enabled, then an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can ignore this notification and proceed with the upgrade.

- b. Verify that the takeover is successful: `storage failover show`

The following example shows that the takeover is successful. Node_A_2 is in the "Waiting for giveback" state and node_A_1 is in the "In takeover" state.

```

cluster1::> storage failover show
                                Takeover
      Node          Partner      Possible State Description
      -----
      -----
node_A_1        node_A_2      false     In takeover
node_A_2        node_A_1      -         Waiting for giveback (HA
mailboxes)
2 entries were displayed.

```

2. Initiate a takeover of the target node on cluster_B:

Do not specify the `-option immediate` parameter, because a normal takeover is required for the nodes that are being taken over to boot onto the new software image.

- Take over the DR partner on cluster_B (node_B_2):

If you are upgrading from...	Enter this command...
ONTAP 9.2 or ONTAP 9.1	<code>storage failover takeover -ofnode node_B_2</code>
ONTAP 9.0 or Data ONTAP 8.3.x	<code>storage failover takeover -ofnode node_B_2 -option allow-version-mismatch</code> The <code>allow-version-mismatch</code> option is not required for upgrades from ONTAP 9.0 to ONTAP 9.1 or for any patch upgrades.

The node boots up to the "Waiting for giveback" state.



If AutoSupport is enabled, an AutoSupport message is sent indicating that the nodes are out of cluster quorum. You can safely ignore this notification and proceed with the upgrade.

- Verify that the takeover is successful: `storage failover show`

The following example shows that the takeover is successful. Node_B_2 is in the "Waiting for giveback" state and node_B_1 is in the "In takeover" state.

```

cluster1::> storage failover show
                           Takeover
      Node          Partner      Possible State Description
      -----
      -----
node_B_1        node_B_2      false    In takeover
node_B_2        node_B_1      -       Waiting for giveback (HA
mailboxes)
2 entries were displayed.

```

3. Wait at least eight minutes to ensure the following conditions:

- Client multipathing (if deployed) is stabilized.
- Clients are recovered from the pause in I/O that occurs during takeover.

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

4. Return the aggregates to the target nodes:

After upgrading MetroCluster IP configurations to ONTAP 9.5, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

- a. Give back the aggregates to the DR partner on cluster_A: `storage failover giveback -ofnode node_A_2`
- b. Give back the aggregates to the DR partner on cluster_B: `storage failover giveback -ofnode node_B_2`

The giveback operation first returns the root aggregate to the node and then, after the node has finished booting, returns the non-root aggregates.

5. Verify that all aggregates have been returned by issuing the following command on both clusters: `storage failover show-giveback`

If the Giveback Status field indicates that there are no aggregates to give back, then all aggregates have been returned. If the giveback is vetoed, the command displays the giveback progress and which subsystem vetoed the giveback.

6. If any aggregates have not been returned, do the following:

- a. Review the veto workaround to determine whether you want to address the “veto” condition or override the veto.
- b. If necessary, address the “veto” condition described in the error message, ensuring that any identified operations are terminated gracefully.
- c. Reenter the storage failover giveback command.

If you decided to override the “veto” condition, set the `-override-veto`s parameter to true.

7. Wait at least eight minutes to ensure the following conditions:

- Client multipathing (if deployed) is stabilized.

- Clients are recovered from the pause in I/O that occurs during giveback.

The recovery time is client-specific and might take longer than eight minutes depending on the characteristics of the client applications.

- Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

- Confirm the version on cluster_A: `system image show`

The following example shows that System image2 (target ONTAP image) is the default and current version on node_A_2:

```
cluster_B::*> system image show
      Is      Is
      Node    Image  Default Current Version   Install
                                         Date
-----
node_A_1
      image1  false  false    X.X.X  MM/DD/YYYY TIME
      image2  true   true    Y.Y.Y  MM/DD/YYYY TIME
node_A_2
      image1  false  false    X.X.X  MM/DD/YYYY TIME
      image2  true   true    Y.Y.Y  MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

- Confirm the version on cluster_B: `system image show`

The following example shows that System image2 (target ONTAP image) is the default and current version on node_B_2:

```

cluster_B::> system image show
          Is      Is
          Node    Image  Default Current Version   Install
          -----  -----  -----  -----
node_B_1
          image1  false  false    X.X.X    MM/DD/YYYY TIME
          image2  true   true    Y.Y.Y    MM/DD/YYYY TIME
node_B_2
          image1  false  false    X.X.X    MM/DD/YYYY TIME
          image2  true   true    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>

```

11. For each node in the HA pair, enable automatic giveback: `storage failover modify -node target-node -auto-giveback true`

This command must be repeated for each node in the HA pair.

12. Verify that automatic giveback is enabled: `storage failover show -fields auto-giveback`

This example shows that automatic giveback has been enabled on both nodes:

```

cluster_x::> storage failover show -fields auto-giveback
          node      auto-giveback
          -----
node_x_1  true
node_x_2  true
2 entries were displayed.

```

Manual nondisruptive upgrade of a two-node MetroCluster configuration in ONTAP 9.2 or earlier using the CLI

You can upgrade ONTAP nondisruptively for a two-node MetroCluster configuration. This method has several steps: initiating a negotiated switchover, updating the cluster at the “failed” site, initiating switchback, and then repeating the process on the cluster at the other site.

This procedure is for two-node MetroCluster configurations running ONTAP 9.2 or earlier only.

+
Do not use this procedure if you have a four-node MetroCluster configuration.

+
If you have a two-node MetroCluster configuration running ONTAP 9.3 or later, perform an [automated nondisruptive upgrade using System Manager](#).

1. Set the privilege level to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

2. On the cluster to be upgraded, install the new ONTAP software image as the default: `system node image update -package package_location -setDefault true -replace-package true`

```
cluster_B::*> system node image update -package  
http://www.example.com/NewImage.tgz -setDefault true -replace-package  
true
```

3. Verify that the target software image is set as the default image: `system node image show`

The following example shows that `NewImage` is set as the default image:

```
cluster_B::*> system node image show  
          Is      Is  
Node     Image    Default Current Version      Install  
-----  
-----  
node_B_1  
          OldImage  false   true    X.X.X      MM/DD/YYYY TIME  
          NewImage   true   false   Y.Y.Y      MM/DD/YYYY TIME  
2 entries were displayed.
```

4. If the target software image is not set as the default image, then change it: `system image modify { -node * -iscurrent false} -isdefault true`
5. Verify that all cluster SVMs are in a health state: `metrocluster vserver show`
6. On the cluster that is not being updated, initiate a negotiated switchover: `metrocluster switchover`

The operation can take several minutes. You can use the metrocluster operation show command to verify that the switchover is completed.

In the following example, a negotiated switchover is performed on the remote cluster ("cluster_A"). This causes the local cluster ("cluster_B") to halt so that you can update it.

```
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".
Do you want to continue? {y|n}: y
```

7. Verify that all cluster SVMs are in a health state: `metrocluster vserver show`
8. Resynchronize the data aggregates on the “surviving” cluster: `metrocluster heal -phase aggregates`

After upgrading MetroCluster IP configurations to ONTAP 9.5 or later, the aggregates will be in a degraded state for a short period before resynchronizing and returning to a mirrored state.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. Verify that the healing operation was completed successfully: `metrocluster operation show`

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Resynchronize the root aggregates on the “surviving” cluster: `metrocluster heal -phase root-aggregates`

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Verify that the healing operation was completed successfully: `metrocluster operation show`

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. On the halted cluster, boot the node from the LOADER prompt: `boot_ontap`
13. Wait for the boot process to finish, and then verify that all cluster SVMs are in a health state: `metrocluster vserver show`
14. Perform a switchback from the “surviving” cluster: `metrocluster switchback`
15. Verify that the switchback was completed successfully: `metrocluster operation show`

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Verify that all cluster SVMs are in a health state: `metrocluster vserver show`
17. Repeat all previous steps on the other cluster.
18. Verify that the MetroCluster configuration is healthy:
 - a. Check the configuration: `metrocluster check run`

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
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.

- b. If you want to view more detailed results, use the metrocluster check run command: `metrocluster check aggregate showmetrocluster check config-replication showmetrocluster check lif show``metrocluster check node show`
- c. Set the privilege level to advanced: `set -privilege advanced`
- d. Simulate the switchover operation: `metrocluster switchover -simulate`
- e. Review the results of the switchover simulation: `metrocluster operation show`

```
cluster_A::*> metrocluster operation show
    Operation: switchover
        State: successful
    Start time: MM/DD/YYYY TIME
    End time: MM/DD/YYYY TIME
    Errors: -
```

- f. Return to the admin privilege level: `set -privilege admin`
- g. Repeat these substeps on the other cluster.

You should perform any post-upgrade tasks.

Related information

[MetroCluster Disaster recovery](#)

Manual disruptive upgrade using the CLI

If you can take your cluster offline to upgrade to a new ONTAP release, then you can use the disruptive upgrade method. This method has several steps: disabling storage failover for each HA pair, rebooting each node in the cluster, and then reenabling storage failover.

- You must have satisfied preparation requirements.
- If you are operating in a SAN environment, all SAN clients must be shut down or suspended until the upgrade is complete.

If SAN clients are not shut down or suspended prior to a disruptive upgrade , then the client file systems and applications suffer errors that might require manual recovery after the upgrade is completed.

In a disruptive upgrade, downtime is required because storage failover is disabled for each HA pair, and each node is updated. When storage failover is disabled, each node behaves as a single-node cluster; that is, system services associated with the node are interrupted for as long as it takes the system to reboot.

1. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`
The advanced prompt (***>**) appears.
2. Set the new ONTAP software image to be the default image: `system image modify {-node * -iscurrent false} -isdefault true`

This command uses an extended query to change the target ONTAP software image (which is installed as the alternate image) to be the default image for each node.

3. Verify that the new ONTAP software image is set as the default image: `system image show`

In the following example, image 2 is the new ONTAP version and is set as the default image on both nodes:

```
cluster1::>*> system image show
      Is      Is
      Node   Image  Default Current Version   Install
-----  -----  -----  -----
node0
      image1  false   true    X.X.X   MM/DD/YYYY TIME
      image2  true    false   Y.Y.Y   MM/DD/YYYY TIME
node1
      image1  false   true    X.X.X   MM/DD/YYYY TIME
      image2  true    false   Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.
```

4. Perform either one of the following steps:

If the cluster consists of...	Do this...
One node	Continue to the next step.
Two nodes	<ol style="list-style-type: none">Disable cluster high availability: <code>cluster ha modify -configured false</code> Enter <code>y</code> to continue when prompted.Disable storage failover for the HA pair: <code>storage failover modify -node * -enabled false</code>
More than two nodes	Disable storage failover for each HA pair in the cluster: <code>storage failover modify -node * -enabled false</code>

5. Reboot a node in the cluster: `system node reboot -node nodename -ignore-quorum-warnings`



Do not reboot more than one node at a time.

The node boots the new ONTAP image. The ONTAP login prompt appears, indicating that the reboot process is complete.

6. After the node or set of nodes has rebooted with the new ONTAP image, confirm that the new software is running: `system node image show`

In the following example, image1 is the new ONTAP version and is set as the current version on node0:

```
cluster1::*> system node image show
      Is      Is
      Node    Image  Default Current Version   Install
                                         Date
-----
node0
      image1  true   true    X.X.X      MM/DD/YYYY TIME
      image2  false  false    Y.Y.Y      MM/DD/YYYY TIME
node1
      image1  true   false   X.X.X      MM/DD/YYYY TIME
      image2  false  true    Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.
```

7. Verify that the upgrade is completed successfully:

- Set the privilege level to advanced: `set -privilege advanced`
- Verify that the upgrade status is complete for each node: `system node upgrade-revert show -node nodename`

The status should be listed as complete.

If the upgrade is not successful, from the node, run the `system node upgrade-revert upgrade` command. If this command does not complete the node's upgrade, contact technical support immediately.

- Return to the admin privilege level: `set -privilege admin`

8. Repeat Steps 2 through 7 for each additional node.

9. If the cluster consists of two or more nodes, enable storage failover for each HA pair in the cluster:
`storage failover modify -node * -enabled true`
10. If the cluster consists of only two nodes, enable cluster high availability: `cluster ha modify -configured true`

What to do after upgrading

After upgrading your ONTAP software, there are several tasks you should perform to verify your cluster readiness.

Post-upgrade cluster verification

After you upgrade you should verify your cluster version, cluster health, and storage health.

Verify cluster version

After all of the HA pairs have been upgraded, you must use the `version` command to verify that all of the nodes are running the target release.

The cluster version is the lowest version of ONTAP running on any node in the cluster. If the cluster version is not the target ONTAP release, you can upgrade your cluster.

1. Verify that the cluster version is the target ONTAP release: `version`
2. If the cluster version is not the target ONTAP release, you can verify the upgrade status of all nodes `system node upgrade-revert show`

Verify cluster health

After you upgrade a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node          Health  Eligibility
-----
node0         true    true
node1         true    true
```

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Enter `y` to continue.
4. Verify the configuration details for each RDB process.
 - The relational database epoch and database epochs should match for each node.
 - The per-ring quorum master should be the same for all nodes.

Note that each ring might have a different quorum master.

To display this RDB process...	Enter this command...
Management application	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

This example shows the volume location database process:

```

cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch     DB Epoch DB Trnxs Master     Online
-----  -----  -----  -----  -----  -----  -----
node0    vldb     154      154      14847   node0    master
node1    vldb     154      154      14847   node0    secondary
node2    vldb     154      154      14847   node0    secondary
node3    vldb     154      154      14847   node0    secondary
4 entries were displayed.

```

5. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -messagename scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```

cluster1::*> event log show -messagename scsiblade.*
Time          Node          Severity      Event
-----  -----
-----  -----
MM/DD/YYYY TIME  node0          INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1          INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...

```

6. Return to the admin privilege level: `set -privilege admin`

Related information

[System administration](#)

Verify storage health

After you upgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:

To check for...	Do this...
Broken disks	<ul style="list-style-type: none"> a. Display any broken disks: <code>storage disk show -state broken</code> b. Remove or replace any broken disks.

To check for...	Do this...
Disks undergoing maintenance or reconstruction	<p>a. Display any disks in maintenance, pending, or reconstructing states: <code>storage disk show -state maintenance pending reconstructing</code></p> <p>b. Wait for the maintenance or reconstruction operation to finish before proceeding.</p>

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you proceed with the upgrade.

Related information

Disk and aggregate management

Verify all LIFs are on home ports after upgrade

During a reboot, some LIFs might have been migrated to their assigned failover ports. After you upgrade a cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

1. Display the status of all LIFs: `network interface show`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0
      Logical      Status      Network      Current      Current  Is
Vserver   Interface  Admin/Oper Address/Mask    Node       Port   Home
-----
vs0
  data001    down/down  192.0.2.120/24  node0     e0e    true
  data002    down/down  192.0.2.121/24  node0     e0f    true
  data003    down/down  192.0.2.122/24  node0     e2a    true
  data004    down/down  192.0.2.123/24  node0     e2b    true
  data005    down/down  192.0.2.124/24  node0     e0e   false
  data006    down/down  192.0.2.125/24  node0     e0f   false
  data007    down/down  192.0.2.126/24  node0     e2a   false
  data008    down/down  192.0.2.127/24  node0     e2b   false
8 entries were displayed.
```

If any LIFs appear with a Status Admin status of "down" or with an Is home status of "false", continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

```
cluster1::> network interface revert *
8 entries were acted on.
```

4. Verify that all LIFs are in their home ports: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.

```

cluster1::> network interface show -vserver vs0
      Logical      Status      Network          Current   Current Is
Vserver  Interface  Admin/Oper Address/Mask    Node     Port   Home
-----
vs0
      data001    up/up     192.0.2.120/24  node0    e0e    true
      data002    up/up     192.0.2.121/24  node0    e0f    true
      data003    up/up     192.0.2.122/24  node0    e2a    true
      data004    up/up     192.0.2.123/24  node0    e2b    true
      data005    up/up     192.0.2.124/24  node1    e0e    true
      data006    up/up     192.0.2.125/24  node1    e0f    true
      data007    up/up     192.0.2.126/24  node1    e2a    true
      data008    up/up     192.0.2.127/24  node1    e2b    true
8 entries were displayed.

```

Post upgrade checks for special configurations

If your cluster is configured with any of the following features you might need to perform additional steps after you upgrade.

Ask yourself...	If your answer is yes, then do this...
Did I upgrade to ONTAP 9.8 or later from ONTAP 9.7 or earlier?	Verify your network configuration
Do I have a MetroCluster configuration?	Verify your networking and storage status
Do I have a SAN configuration?	Verify your SAN configuration
Am I using NetApp Storage Encryption and I upgraded to ONTAP 9.3 or later?	Reconfigure KMIP server connections
Do I have load-sharing mirrors?	Relocate moved load-sharing mirror source volumes
Am I using SnapMirror?	Resume SnapMirror operations
Did I upgrade from ONTAP 8.3.0?	Set the desired NT ACL permissions display level for NFS clients
Do I have administrator accounts created prior to ONTAP 9.0?	Enforce SHA-2 on administrator passwords

Verifying your network configuration after upgrade

ONTAP 9.8 and later automatically monitors layer 2 reachability. After you upgrade from ONTAP 9.7x or earlier to ONTAP 9.8 or later, you should verify that each .network port has reachability to its expected broadcast domain.

1. Verify each port has reachability to its expected domain:[network port reachability show -detail](#)

A reachability-status of ok indicates that the port has layer 2 reachability to its assigned domain.

Verify networking and storage status for MetroCluster configurations

After performing an update in a MetroCluster configuration, you should verify the status of the LIFs, aggregates, and volumes for each cluster.

1. Verify the LIF status: `network interface show`

In normal operation, LIFs for source SVMs must have an admin status of up and be located on their home nodes. LIFs for destination SVMs are not required to be up or located on their home nodes. In switchover, all LIFs have an admin status of up, but they do not need to be located on their home nodes.

```
cluster1::> network interface show
      Logical      Status      Network          Current
      Current Is
      Vserver      Interface   Admin/Oper Address/Mask      Node      Port
      Home
      -----
      -----
      Cluster
            cluster1-a1_clus1
                  up/up      192.0.2.1/24      cluster1-01
                                         e2a
      true
            cluster1-a1_clus2
                  up/up      192.0.2.2/24      cluster1-01
                                         e2b
      true

      cluster1-01
            clus_mgmt      up/up      198.51.100.1/24      cluster1-01
                                         e3a
      true
            cluster1-a1_inet4_intercluster1
                  up/up      198.51.100.2/24      cluster1-01
                                         e3c
      true
            ...
27 entries were displayed.
```

2. Verify the state of the aggregates: `storage aggregate show -state !online`

This command displays any aggregates that are *not* online. In normal operation, all aggregates located at the local site must be online. However, if the MetroCluster configuration is in switchover, root aggregates at

the disaster recovery site are permitted to be offline.

This example shows a cluster in normal operation:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

This example shows a cluster in switchover, in which the root aggregates at the disaster recovery site are offline:

```
cluster1::> storage aggregate show -state !online
Aggregate      Size Available Used% State    #Vols  Nodes      RAID
Status
-----
-----
aggr0_b1
          0B        0B     0% offline      0 cluster2-01
  raid_dp,
  mirror

degraded
aggr0_b2
          0B        0B     0% offline      0 cluster2-02
  raid_dp,
  mirror

degraded
2 entries were displayed.
```

3. Verify the state of the volumes: `volume show -state !online`

This command displays any volumes that are *not* online.

If the MetroCluster configuration is in normal operation (it is not in switchover state), the output should show all volumes owned by the cluster's secondary SVMs (those with the SVM name appended with "-mc").

Those volumes come online only in the event of a switchover.

This example shows a cluster in normal operation, in which the volumes at the disaster recovery site are not online.

```

cluster1::> volume show -state !online
  (volume show)
Vserver    Volume      Aggregate   State     Type      Size
Available  Used%
-----  -----
vs2-mc    vol1        agg1_b1    -          RW       -
-
vs2-mc    root_vs2    agg0_b1    -          RW       -
-
vs2-mc    vol2        agg1_b1    -          RW       -
-
vs2-mc    vol3        agg1_b1    -          RW       -
-
vs2-mc    vol4        agg1_b1    -          RW       -
-
5 entries were displayed.

```

- Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you proceed with the upgrade.

Verify the SAN configuration after an upgrade

If you are upgrading in a SAN environment, then after the upgrade, you should verify that each initiator that was connected to a LIF before the upgrade has successfully reconnected to the LIF.

- Verify that each initiator is connected to the correct LIF.

You should compare the list of initiators to the list you made during the upgrade preparation.

For...	Enter...
iSCSI	<code>iscsi initiator show -fields igroup,initiator-name,tpgroup</code>
FC	<code>fcp initiator show -fields igroup,wwpn,lif</code>

Reconfiguring KMIP server connections after upgrading to ONTAP 9.3 or later

After performing an upgrade to ONTAP 9.3 or later, you must reconfigure your external key management (KMIP) server connections.

1. Configure the key manager connectivity: `security key-manager setup`
2. Add your KMIP servers: `security key-manager add -address key_management_server_ip_address`
3. Verify that KMIP servers are connected: `security key-manager show -status`
4. Query the key servers: `security key-manager query`
5. Create a new authentication key and passphrase: `security key-manager create-key -prompt -for-key true`

The passphrase must have a minimum of 32 characters.

6. Query the new authentication key: `security key-manager query`
7. Assign the new authentication key to your self-encrypting disks (SEDs): `storage encryption disk modify -disk disk_ID -data-key-id key_ID`



Make sure you are using the new authentication key from your query.

8. If needed, assign a FIPS key to the SEDs: `storage encryption disk modify -disk disk_id -fips-key-id fips_authentication_key_id`

If your security setup requires you to use different keys for data authentication and FIPS 140-2 authentication, you should create a separate key for each. If that is not the case, you can use the same authentication key for FIPS compliance that you use for data access.

Relocating moved load-sharing mirror source volumes

After successfully completing a nondisruptive upgrade, you can move load-sharing mirror source volumes back to the locations they were in originally before the upgrade.

1. Identify the location to which you are moving the load-sharing mirror source volume by using the record you created before moving the load-sharing mirror source volume.
2. Move the load-sharing mirror source volume back to its original location by using the volume move start command.

Resuming SnapMirror operations

After completing a nondisruptive upgrade, you must resume any SnapMirror relationships that were suspended.

Existing SnapMirror relationships must have been suspended by using the snapmirror quiesce command, and the cluster must have been nondisruptively upgraded.

1. Resume transfers for each SnapMirror relationship that was previously quiesced: `snapmirror resume *`

This command resumes the transfers for all quiesced SnapMirror relationships.

2. Verify that the SnapMirror operations have resumed: `snapmirror show`

```

cluster1::> snapmirror show

Source          Destination   Mirror  Relationship  Total
Last           Path        Type    Path        State   Status      Progress  Healthy
Path           Updated

-----
-----


cluster1-vs1:dp_src1
    DP    cluster1-vs2:dp_dst1
                    Snapmirrored
                    Idle      -       true     -
cluster1-vs1:xdp_src1
    XDP   cluster1-vs2:xdp_dst1
                    Snapmirrored
                    Idle      -       true     -
cluster1://cluster1-vs1/ls_src1
    LS    cluster1://cluster1-vs1/ls_mr1
                    Snapmirrored
                    Idle      -       true     -
cluster1://cluster1-vs1/ls_mr2
    Snapmirrored
                    Idle      -       true     -
4 entries were displayed.

```

For each SnapMirror relationship, verify that the Relationship Status is **Idle**. If the status is **Transferring**, wait for the SnapMirror transfer to complete, and then reenter the command to verify that the status has changed to **Idle**.

For each SnapMirror relationship that is configured to run on a schedule, you should verify that the first scheduled SnapMirror transfer completes successfully.

Setting the desired NT ACL permissions display level for NFS clients

After upgrading from ONTAP 8.3.0, the default handling for displaying NT ACL permissions to NFS clients has changed. You should check the setting and change it to the desired setting for your environment if necessary. This task does not apply if you are upgrading from ONTAP 8.3.1 or later.

In multiprotocol environments, ONTAP displays to NFS clients the permissions of NTFS security-style files and directories based on the access granted by the NT ACL to any user. In ONTAP 8.3.0, ONTAP by default displayed to NFS clients the permission based on the maximum access granted by the NT ACL. After upgrading, the default setting changes to display permissions based on the minimum access granted by the NT ACL. This change applies to new and existing storage virtual machines (SVMs).

1. Set the privilege level to advanced: `set -privilege advanced`

2. Check the setting for displaying NT ACL permissions for NFS clients: `vserver nfs show -vserver vserver_name -fields ntacldisplay-permissive-perms`

After upgrading from 8.3.0, the value for this new parameter is disabled, meaning ONTAP displays the minimum permissions.

3. If you prefer to display the maximum permissions, change the setting individually for each SVM as desired: `vserver nfs modify -vserver vserver_name -ntacldisplay-permissive-perms enabled`

4. Verify that the change took effect: `vserver nfs show -vserver vserver_name -fields ntacldisplay-permissive-perms`

5. Return to the admin privilege level: `set -privilege admin`

Enforcing SHA-2 on administrator account passwords

Administrator accounts created prior to ONTAP 9.0 continue to use MD5 passwords after the upgrade, until the passwords are manually changed. MD5 is less secure than SHA-2. Therefore, after upgrading, you should prompt users of MD5 accounts to change their passwords to use the default SHA-512 hash function.

The password hash functionality enables you to do the following:

- Display user accounts that match the specified hash function.
- Expire accounts that use a specified hash function (for example, MD5), forcing the users to change their passwords in their next login.
- Lock accounts whose passwords use the specified hash function.
- When reverting to a release earlier than ONTAP 9, reset the cluster administrator's own password for it to be compatible with the hash function (MD5) that is supported by the earlier release.

ONTAP accepts pre-hashed SHA-2 passwords only by using NetApp Manageability SDK (security-login-create and security-login-modify-password).

Manageability enhancements

1. Migrate the MD5 administrator accounts to the SHA-512 password hash function:

a. Expire all MD5 administrator accounts: `security login expire-password -vserver * -username * -hash-function md5`

Doing so forces MD5 account users to change their passwords upon next login.

b. Ask users of MD5 accounts to log in through a console or SSH session.

The system detects that the accounts are expired and prompts users to change their passwords. SHA-512 is used by default for the changed passwords.

2. For MD5 accounts whose users do not log in to change their passwords within a period of time, force the account migration:

a. Lock accounts that still use the MD5 hash function (advanced privilege level): `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

After the number of days specified by -lock-after, users cannot access their MD5 accounts.

- b. Unlock the accounts when the users are ready to change their passwords: `security login unlock -vserver vserver_name -username user_name`
- c. Have users log in to their accounts through a console or SSH session and change their passwords when the system prompts them to do so.

When you need to update the Disk Qualification Package

The Disk Qualification Package (DQP) adds full support for newly qualified drives. Before you update drive firmware or add new drive types or sizes to a cluster, you must update the DQP. A best practice is to also update the DQP regularly; for example, every quarter or semi-annually.

You need to download and install the DQP in the following situations:

- Whenever you add a new drive type or size to the node

For example, if you already have 1-TB drives and add 2-TB drives, you need to check for the latest DQP update.

- Whenever you update the disk firmware
- Whenever newer disk firmware or DQP files are available
- Whenever you upgrade to a new version of ONTAP.

The DQP is not updated as part of an ONTAP upgrade.

Related information

[NetApp Downloads: Disk Qualification Package](#)

[NetApp Downloads: Disk Drive Firmware](#)

Revert ONTAP

To transition a cluster to an earlier ONTAP release, you must perform a reversion.

The content in this section will guide you through the steps you should take before and after you revert, including the resources you should read and the necessary pre- and post-revert checks you should perform.



If you need to transition a cluster from ONTAP 9.1 to ONTAP 9.0, you need to use the downgrade procedure documented [here](#).

Do I need technical support to revert?

You can revert without assistance on new or test clusters. You should call technical support to revert production clusters. You should also call technical support if you experience any of the following:

- You are in a production environment and revert fails or you encounter any problems before or after the revert such as:
 - The revert process fails and cannot finish.
 - The revert process finishes, but the cluster is unusable in a production environment.
 - The revert process finishes and the cluster goes into production, but you are not satisfied with its behavior.
- You created volumes in ONTAP 9.5 or later and you need to revert to an earlier version. Volumes using adaptive compression must be uncompressed before reverting.

Revert paths

The version of ONTAP that you can revert to varies based on the version of ONTAP currently running on your nodes. You can use the `system image show` command to determine the version of ONTAP running on each node.

You can revert from...	To...
ONTAP 9.9.1 or 9.9.0	ONTAP 9.8
ONTAP 9.8	ONTAP 9.7
ONTAP 9.7	ONTAP 9.6
ONTAP 9.6	ONTAP 9.5
ONTAP 9.5	ONTAP 9.4
ONTAP 9.4	ONTAP 9.3
ONTAP 9.3	ONTAP 9.2

You can revert from...	To...
ONTAP 9.2	ONTAP 9.1
ONTAP 9.1 or ONTAP 9	Data ONTAP 8.3.x



If you need to change from ONTAP 9.1 TO 9.0, you should follow the [downgrade process](#) documented here.

What should I read before I revert?

Resources to review before you revert

Before you revert ONTAP, you should confirm hardware support and review resources to understand issues you might encounter or need to resolve.

1. Review the [ONTAP 9 Release Notes](#) for the target release.

The “Important cautions” section describes potential issues that you should be aware of before downgrading or reverting.

2. Confirm that your hardware platform is supported in the target release.

[NetApp Hardware Universe](#)

3. Confirm that your cluster and management switches are supported in the target release.

You must verify that the NX-OS (cluster network switches), IOS (management network switches), and reference configuration file (RCF) software versions are compatible with the version of ONTAP to which you are reverting.

[NetApp Downloads: Cisco Ethernet Switch](#)

4. If your cluster is configured for SAN, confirm that the SAN configuration is fully supported.

All SAN components—including target ONTAP software version, host OS and patches, required Host Utilities software, and adapter drivers and firmware—should be supported.

[NetApp Interoperability Matrix Tool](#)

Revert considerations

You need to consider the revert issues and limitations before beginning an ONTAP reversion.

- Reversion is disruptive.

No client access can occur during the reversion. If you are reverting a production cluster, be sure to include this disruption in your planning.

- Reversion affects all nodes in the cluster.

The reversion affects all nodes in the cluster; however, the reversion must be performed and completed on each HA pair before other HA pairs are reverted.

- The reversion is complete when all nodes are running the new target release.

When the cluster is in a mixed-version state, you should not enter any commands that alter the cluster operation or configuration except as necessary to satisfy reversion requirements; monitoring operations are permitted.



If you cannot complete the reversion for any reason, contact technical support immediately. If you have reverted some, but not all of the nodes, do not attempt to upgrade the cluster back to the source release.

- When you revert a node, it clears the cached data in a Flash Cache module.

Because there is no cached data in the Flash Cache module, the node serves initial read requests from disk, which results in decreased read performance during this period. The node repopulates the cache as it serves read requests.

- A LUN that is backed up to tape running on ONTAP 9.x can be restored only to 9.x and later releases and not to an earlier release.
- If your current version of ONTAP supports In-Band ACP (IBACP) functionality, and you revert to a version of ONTAP that does not support IBACP, the alternate path to your disk shelf is disabled.
- If LDAP is used by any of your storage virtual machines (SVMs), LDAP referral must be disabled before reversion.
- In MetroCluster IP systems using switches which are MetroCluster compliant but not MetroCluster validated, the reversion from ONTAP 9.7 to 9.6 is disruptive as there is no support for systems using ONTAP 9.6 and earlier.

Things to verify before you revert

Before revert, you should verify your cluster health, storage health, and system time. You should also delete any cluster jobs that are running and gracefully terminate any CIFS sessions that are not continuously available.

Verify cluster health

Before you revert cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum.

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node          Health  Eligibility
-----
node0        true    true
node1        true    true
```

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Enter `y` to continue.
4. Verify the configuration details for each RDB process.
 - The relational database epoch and database epochs should match for each node.
 - The per-ring quorum master should be the same for all nodes.

Note that each ring might have a different quorum master.

To display this RDB process...	Enter this command...
Management application	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

This example shows the volume location database process:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch      DB Epoch DB Trnxs Master      Online
-----  -----
node0      vldb     154       154      14847   node0    master
node1      vldb     154       154      14847   node0    secondary
node2      vldb     154       154      14847   node0    secondary
node3      vldb     154       154      14847   node0    secondary
4 entries were displayed.
```

1. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -messagename scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```

cluster1::> event log show -messagename scsiblade.*
Time           Node          Severity      Event
-----
----- MM/DD/YYYY TIME   node0          INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME   node1          INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...

```

2. Return to the admin privilege level: `set -privilege admin`

Related information

System administration

Verify storage health

Before you revert a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:

To check for...	Do this...
Broken disks	<ul style="list-style-type: none"> a. Display any broken disks: <code>storage disk show -state broken</code> b. Remove or replace any broken disks.
Disks undergoing maintenance or reconstruction	<ul style="list-style-type: none"> a. Display any disks in maintenance, pending, or reconstructing states: <code>storage disk show -state maintenance pending reconstructing</code> b. Wait for the maintenance or reconstruction operation to finish before proceeding.

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```

cluster1::> storage aggregate show -state !online
There are no entries matching your query.

```

3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online  
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you proceed with the upgrade.

Related information

[Disk and aggregate management](#)

Verifying the system time

Before you revert, you should verify that NTP is configured, and that the time is synchronized across the cluster.

1. Verify that the cluster is associated with an NTP server: `cluster time-service ntp server show`
2. Verify that each node has the same date and time: `cluster date show`

```
cluster1::> cluster date show  
Node          Date                Timezone  
-----  
node0         4/6/2013 20:54:38    GMT  
node1         4/6/2013 20:54:38    GMT  
node2         4/6/2013 20:54:38    GMT  
node3         4/6/2013 20:54:38    GMT  
4 entries were displayed.
```

Verify that no jobs are running

Before you revert the ONTAP software, you must verify the status of cluster jobs. If any aggregate, volume, NDMP (dump or restore), or Snapshot jobs (such as create, delete, move, modify, replicate, and mount jobs) are running or queued, you must allow the jobs to finish successfully or stop the queued entries.

1. Review the list of any running or queued aggregate, volume, or Snapshot jobs: `job show`

```

cluster1::> job show
          Owning
Job ID Name           Vserver   Node     State
-----
8629   Vol Reaper      cluster1   -        Queued
       Description: Vol Reaper Job
8630   Certificate Expiry Check
                           cluster1   -        Queued
       Description: Certificate Expiry Check
.
.
.

```

2. Delete any running or queued aggregate, volume, or Snapshot copy jobs: `job delete -id job_id`

```
cluster1::> job delete -id 8629
```

3. Verify that no aggregate, volume, or Snapshot jobs are running or queued: `job show`

In this example, all running and queued jobs have been deleted:

```

cluster1::> job show
          Owning
Job ID Name           Vserver   Node     State
-----
9944   SnapMirrorDaemon_7_2147484678
                           cluster1   node1     Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                           cluster1   node0     Dormant
       Description: SnapMirror Service Job
2 entries were displayed

```

CIFS sessions that should be terminated

Before you revert, you should identify and gracefully terminate any CIFS sessions that are not continuously available.

Continuously available CIFS shares, which are accessed by Hyper-V or Microsoft SQL Server clients using the SMB 3.0 protocol, do not need to be terminated before upgrading or downgrading.

1. Identify any established CIFS sessions that are not continuously available: `vserver cifs session show -continuously-available Yes -instance`

This command displays detailed information about any CIFS sessions that have no continuous availability. You should terminate them before proceeding with the ONTAP downgrade.

```
cluster1::> vserver cifs session show -continuously-available Yes  
-instance  
  
          Node: node1  
          Vserver: vs1  
          Session ID: 1  
          Connection ID: 4160072788  
Incoming Data LIF IP Address: 198.51.100.5  
          Workstation IP address: 203.0.113.20  
Authentication Mechanism: NTLMv2  
          Windows User: CIFSLAB\user1  
          UNIX User: nobody  
          Open Shares: 1  
          Open Files: 2  
          Open Other: 0  
Connected Time: 8m 39s  
          Idle Time: 7m 45s  
Protocol Version: SMB2_1  
Continuously Available: No  
1 entry was displayed.
```

2. If necessary, identify the files that are open for each CIFS session that you identified: `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1  
  
          Node:      node1  
          Vserver:    vs1  
          Connection: 4160072788  
          Session:    1  
File     File      Open Hosting  
Continuously  
ID       Type      Mode Volume      Share           Available  
----- ----- ----- -----  
-----  
1       Regular    rw   vol10      homedirshare      No  
Path: \TestDocument.docx  
2       Regular    rw   vol10      homedirshare      No  
Path: \file1.txt  
2 entries were displayed.
```

Pre-revert checks

Depending on your environment, you need to consider certain factors before revert. Get started by reviewing the table below to see what special considerations you need to consider.

Ask yourself...	If your answer is yes, then do this...
Is my cluster running SnapMirror?	<ul style="list-style-type: none">Review considerations for reverting systems with SnapMirror Synchronous relationshipsReview reversion requirements for SnapMirror and SnapVault relationships
Is my cluster running SnapLock?	Set autocommit periods
Do I have Split FlexClone volumes?	Reverse physical block sharing
Do I have FlexGroup volumes?	Disable qtree functionality
Do I have CIFS servers in workgroup mode?	Move or delete CIFS servers in workgroup mode
Do I have deduplicated volumes?	Verify volume contains enough free space
Do I have a 2 or 4-node MetroCluster configuration?	Disable automatic unplanned switchover
Do I have Snapshot copies?	Prepare Snapshot copies

SnapMirror

Considerations for reverting systems with SnapMirror Synchronous relationships

You must be aware of the considerations for SnapMirror Synchronous relationships before reverting from ONTAP 9.6 to ONTAP 9.5.

Before reverting, you must take the following steps if you have SnapMirror Synchronous relationships:

- You must delete any SnapMirror Synchronous relationship in which the source volume is serving data using NFSv4 or SMB/CIFS.

ONTAP 9.5 does not support NFSv4 and SMB/CIFS.

- You must delete any SnapMirror Synchronous relationships in a mirror-mirror cascade deployment.

A mirror-mirror cascade deployment is not supported for SnapMirror Synchronous relationships in ONTAP 9.5.

- If the common Snapshot copies in ONTAP 9.5 are not available during revert, you must initialize the SnapMirror Synchronous relationship after reverting.

After two hours of upgrade to ONTAP 9.6, the common Snapshot copies from ONTAP 9.5 are automatically replaced by the common Snapshot copies in ONTAP 9.6. Therefore, you cannot resynchronize the SnapMirror Synchronous relationship after reverting if the common Snapshot copies from ONTAP 9.5 are not available.

Reversion requirements for SnapMirror and SnapVault relationships

The system node revert-to command notifies you of any SnapMirror and SnapVault relationships that need to be deleted or reconfigured for the reversion process to be completed. However, you should be aware of these requirements before you begin the reversion.

- All SnapVault and data protection mirror relationships must be quiesced and then broken.

After the reversion is completed, you can resynchronize and resume these relationships if a common Snapshot copy exists.

- SnapVault relationships must not contain the following SnapMirror policy types:

- async-mirror

You must delete any relationship that uses this policy type.

- MirrorAndVault

If any of these relationships exist, you should change the SnapMirror policy to mirror-vault.

- All load-sharing mirror relationships and destination volumes must be deleted.
- SnapMirror relationships with FlexClone destination volumes must be deleted.
- Network compression must be disabled for each SnapMirror policy.
- The all_source_snapshot rule must be removed from any async-mirror type SnapMirror policies.



The Single File Snapshot Restore (SFSR) and Partial File Snapshot Restore (PFSR) operations are deprecated on the root volume.

- Any currently running single file and Snapshot restore operations must be completed before the reversion can proceed.

You can either wait for the restore operation to finish, or you can abort it.

- Any incomplete single file and Snapshot restore operations must be removed by using the snapmirror restore command.

Set autocommit periods for SnapLock volumes before reverting

To revert from ONTAP 9, the value of the autocommit period for SnapLock volumes must be set in hours, not days. Before attempting to revert, you must check the autocommit value for your SnapLock volumes and modify it from days to hours, if necessary.

1. Verify that there are SnapLock volumes in the cluster that have unsupported autocommit periods:
`volume snaplock show -autocommit-period *days`
2. Modify the unsupported autocommit periods to hours:
`volume snaplock modify -vserver vserver_name -volume volume_name -autocommit-period value hours`

Reverse physical block sharing in split FlexClone volumes

If you have split a FlexClone volume from its parent volume, you must undo the sharing of any physical block between the clone and its parent volume before reverting from ONTAP 9.4 or later to an earlier version of ONTAP.

This task is applicable only for AFF systems when split has been run on any of the FlexClone volumes.

1. Log in to the advanced privilege level: `set -privilege advanced`
2. Identify the split FlexClone volumes with shared physical blocks: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
Node          Vserver    Volume        Aggregate
-----
node1         vs1        vol_clone1   aggr1
node2         vs2        vol_clone2   aggr2
2 entries were displayed.
```

3. Undo the physical block sharing in all of the split FlexClone volumes across the cluster: `volume clone sharing-by-split undo start-all`
4. Verify that there are no split FlexClone volumes with shared physical blocks: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
This table is currently empty.
```

Disable qtree functionality in FlexGroup volumes before reverting

Qtrees for FlexGroup volumes are not supported prior to ONTAP 9.3. You must disable the qtree functionality on FlexGroup volumes before reverting from ONTAP 9.3 to an earlier version of ONTAP.

The qtree functionality is enabled either when you create a qtree or if you modify the security-style and oplock-mode attributes of the default qtree.

1. Identify and delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality:
 - a. Log in to the advanced privilege level: `set -privilege advanced`
 - b. Verify if any FlexGroup volume is enabled with the qtree functionality.

For ONTAP 9.6 or later, use: `volume show is-qtree-caching-enabled true`

For ONTAP 9.5 or earlier, use: `volume show -is-flexgroup-qtree-enabled true`

```

cluster1::*> volume show -is-flexgroup-qtree-enabled true
Vserver      Volume       Aggregate     State      Type      Size
Available    Used%
-----
----- -
vs0          fg           -            online    RW        320MB
220.4MB     31%

```

- c. Delete all of the non-default qtrees in each FlexGroup volume that are enabled with the qtree functionality: `volume qtree delete -vserver svm_name -volume volume_name -qtree qtree_name`

If the qtree functionality is enabled because you modified the attributes of the default qtree and if you do not have any qtrees, you can skip this step.

```

cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree
qtree4
WARNING: Are you sure you want to delete qtree qtree4 in volume fg
vserver vs0? {y|n}: y
[Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.

```

2. Disable the qtree functionality on each FlexGroup volume: `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtree-disable -vserver vs0 -volume fg
```

3. Identify and delete any Snapshot copies that are enabled with the qtree functionality.

- a. Verify if any Snapshot copies are enabled with the qtree functionality: `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtree-enabled`

```

cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtree-enabled
vserver volume snapshot is-flexgroup-qtree-enabled
-----
----- -
vs0      fg      fg_snap1 true
vs0      fg      daily.2017-09-27_0010 true
vs0      fg      daily.2017-09-28_0010 true
vs0      fg      snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true

```

- b. Delete all of the Snapshot copies that are enabled with the qtree functionality: `volume snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true`

The Snapshot copies that must be deleted include regular Snapshot copies and the Snapshot copies taken for SnapMirror relationships. If you have created any SnapMirror relationship for the FlexGroup volumes with a destination cluster that is running ONTAP 9.2 or earlier, you must delete all of the Snapshot copies that were taken when the source FlexGroup volume was enabled for the qtree functionality.

```
cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot daily.2017-09-27_0010 -force true -ignore-owners true
```

Related information

[FlexGroup volumes management](#)

Identify and move CIFS servers in workgroup mode

Before performing a revert, you must delete any CIFS servers in workgroup mode or move them in to a domain. Workgroup mode is not supported on ONTAP versions prior to ONTAP 9.

1. Identify any CIFS servers with a Authentication Style of workgroup: `vserver cifs show`
2. Move or delete the servers you identified:

If you are going to...	Then use this command....
Move the CIFS server from the workgroup to an Active Directory domain:	<code>vserver cifs modify -vserver vserver_name -domain domain_name</code>
Delete the CIFS server	<code>vserver cifs delete -vserver vserver_name</code>

3. If you deleted the CIFS server, enter the username of the domain, then enter the user password.

Related information

[SMB/CIFS management](#)

Verify deduplicated volumes have enough free space before reverting

Before reverting from any version of ONTAP 9, you must ensure that the volumes contain sufficient free space for the revert operation.

The volume must have enough space to accommodate the savings that were achieved through the inline detection of blocks of zeros. For information about the space required, contact technical support.

Reverting from ONTAP 9 on a system that has deduplication enabled includes running advanced mode commands. You must contact technical support for assistance.

If you have enabled both deduplication and data compression on a volume that you want to revert, then you must revert data compression before reverting deduplication.

1. Use the volume efficiency show command with the -fields option to view the progress of the efficiency operations that are running on the volumes.

The following command displays the progress of efficiency operations: `volume efficiency show -fields vserver,volume,progress`

2. Use the volume efficiency stop command with the -all option to stop all active and queued deduplication operations.

The following command stops all active and queued deduplication operations on volume VolA: `volume efficiency stop -vserver vs1 -volume VolA -all`

3. Use the set -privilege advanced command to log in at the advanced privilege level.
4. Use the volume efficiency revert-to command with the -version option to downgrade the efficiency metadata of a volume to a specific version of ONTAP.

The following command reverts the efficiency metadata on volume VolA to ONTAP 9.x: `volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x`



The volume efficiency revert-to command reverts volumes that are present on the node on which this command is executed. This command does not revert volumes across nodes.

5. Use the volume efficiency show command with the -op-status option to monitor the progress of the downgrade.

The following command monitors and displays the status of the downgrade: `volume efficiency show -vserver vs1 -op-status Downgrading`

6. If the revert does not succeed, use the volume efficiency show command with the -instance option to see why the revert failed.

The following command displays detailed information about all fields: `volume efficiency show -vserver vs1 -volume vol1 - instance`

7. After the revert operation is complete, return to the admin privilege level: `set -privilege admin`

Logical storage management

Disable automatic unplanned switchover before reverting two-node and four-node MetroCluster configurations

Before reverting a two-node or four-node MetroCluster configuration, you must disable automatic unplanned switchover (AUSO).

1. On both the clusters in MetroCluster, disable automatic unplanned switchover: `metrocluster modify -auto-switchover-failure-domain auso-disabled`

Related information

[MetroCluster management and disaster recovery](#)

Prepare Snapshot copies before reverting

Before reverting to an earlier ONTAP release, you must disable all Snapshot copy policies and delete any Snapshot copies that were created after upgrading to the current release.

If you are reverting in a SnapMirror environment, you must first have deleted the following mirror relationships:

- All load-sharing mirror relationships
 - Any data protection mirror relationships that were created in ONTAP 8.3.x
 - All data protection mirror relationships if the cluster was re-created in ONTAP 8.3.x
1. Disable Snapshot copy policies for all data SVMs: `volume snapshot policy modify -vserver * -enabled false`
 2. Disable Snapshot copy policies for each node's aggregates:
 - a. Identify the node's aggregates by using the `run -node nodename aggr status` command.
 - b. Disable the Snapshot copy policy for each aggregate: `run -node nodename aggr options aggr_name nosnap on`
 - c. Repeat this step for each remaining node.
 3. Disable Snapshot copy policies for each node's root volume:
 - a. Identify the node's root volume by using the `run -node nodename vol status` command output.

```
vs1::> run -node node1 vol status

      Volume State          Status           Options
          vol0 online    raid_dp, flex   root, nvfail=on
                           64-bit
```

- b. Disable the Snapshot copy policy on the root volume: `run -node nodename vol options root_volume_name nosnap on`
- c. Repeat this step for each remaining node.
4. Delete all Snapshot copies that were created after upgrading to the current release:
 - a. Set the privilege level to advanced: `set -privilege advanced`
 - b. Disable the snapshots: `snapshot policy modify -vserver * -enabled false`
 - c. Delete the node's newer-version Snapshot copies: `volume snapshot prepare-for-revert -node nodename`

This command deletes the newer-version Snapshot copies on each data volume, root aggregate, and root volume.

If any Snapshot copies cannot be deleted, the command fails and notifies you of any required actions you must take before the Snapshot copies can be deleted. You must complete the required

actions and then rerun the volume snapshot prepare-for-revert command before proceeding to the next step.

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all Snapshot copies that have
the format used by the current version of ONTAP. It will fail if
any Snapshot copy policies are enabled, or
if any Snapshot copies have an owner. Continue? {y|n}: y
```

d. Verify that the Snapshot copies have been deleted: `volume snapshot show -node nodename`

If any newer-version Snapshot copies remain, force them to be deleted: `volume snapshot delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore -owners -force`

e. Repeat this step c for each remaining node.

f. Return to the admin privilege level: `set -privilege admin`



You must perform these steps on both the clusters in MetroCluster configuration.

Download and install the ONTAP software image

You must first download the ONTAP software from the NetApp Support site; then you can install it.

Download the software image

To downgrade or revert from ONTAP 9.4 and later, you can copy the ONTAP software image from the NetApp Support Site to a local folder. For a downgrade or revert to ONTAP 9.3 or earlier, you must copy the ONTAP software image to an HTTP server or FTP server on your network.

You should note the following important information:

- Software images are specific to platform models.

You must obtain the correct image for your cluster. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site.

- Software images include the latest version of system firmware that was available when a given version of ONTAP was released.
- If you are downgrading a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must download the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to downgrade or revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

1. Locate the target ONTAP software in the [Software Downloads](#) area of the NetApp Support Site.

2. Copy the software image.

- For ONTAP 9.3 or earlier, copy the software image (for example, 93_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served.
- For ONTAP 9.4 or later, copy the software image (for example, 97_q_image.tgz) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served or to a local folder.

Install the software image

You must install the target software image on the cluster's nodes.

- If you are downgrading or reverting a system with NetApp Volume Encryption from ONTAP 9.5 or later, you must have downloaded the ONTAP software image for non-restricted countries, which includes NetApp Volume Encryption.

If you use the ONTAP software image for restricted countries to downgrade or revert a system with NetApp Volume Encryption, the system panics and you lose access to your volumes.

1. Set the privilege level to advanced, entering `y` when prompted to continue: `set -privilege advanced`

The advanced prompt (`*>`) appears.

2. Install the software image on the nodes.

This command downloads and installs the software image on all of the nodes simultaneously. To download and install the image on each node one at a time, do not specify the `-background` parameter.

- If you are downgrading or reverting a non-MetroCluster configuration or a two-node MetroCluster configuration:
`system node image update -node * -package location -replace-package true -setdefault true -background true`

This command uses an extended query to change the target software image, which is installed as the alternate image, to be the default image for the node.

- If you are dowgrading or reverting a four or eight-node MetroCluster configuration, you must issue the following command on both clusters:
`system node image update -node * -package location -replace-package true true -background true -setdefault false`

This command uses an extended query to change the target software image, which is installed as the alternate image on each node.

3. Enter `y` to continue when prompted.

4. Verify that the software image is downloaded and installed on each node: `system node image show-update-progress -node *`

This command displays the current status of the software image download and installation. You should continue to run this command until all nodes report a Run Status of Exited, and an Exit Status of Success.

The `system node image update` command can fail and display error or warning messages. After resolving any errors or warnings, you can run the command again.

This example shows a two-node cluster in which the software image is downloaded and installed successfully on both nodes:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
    Run Status:      Exited
    Exit Status:     Success
    Phase:           Run Script
    Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Revert an ONTAP cluster

To take the cluster offline to revert to an earlier ONTAP release, you must disable storage failover and the data LIFs, address reversion preconditions, revert the cluster and file system configurations on a node, and then repeat the process for each additional node in the cluster.

You must have completed the revert [verifications](#) and [pre-checks](#).

Reverting a cluster requires you to take the cluster offline for the duration of the reversion.

1. Set the privilege level from admin to advanced, entering **y** when prompted to continue: `set -privilege advanced`

The advanced prompt (***>**) appears.

2. Verify that the target ONTAP software is installed: `system image show`

The following example shows that version 9.1 is installed as the alternate image on both nodes:

```

cluster1::*> system image show
          Is      Is
          Default Current Version      Install
Node     Image
----- ----- ----- -----
node0
        image1  true   true    9.2      MM/DD/YYYY TIME
        image2  false  false    9.1      MM/DD/YYYY TIME
node1
        image1  true   true    9.2      MM/DD/YYYY TIME
        image2  false  false    9.1      MM/DD/YYYY TIME
4 entries were displayed.

```

3. Disable all of the data LIFs in the cluster: `network interface modify {-role data} -status -admin down`
4. If the cluster consists of only two nodes, disable cluster HA: `cluster ha modify -configured false`
5. Disable storage failover for the nodes in the HA pair from either node: `storage failover modify -node nodename -enabled false`

You only need to disable storage failover once for the HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

6. Log in to the node that you want to revert.

To revert a node, you must be logged in to the cluster through the node's node management LIF.

7. Set the node's target ONTAP software image to be the default image: `system image modify -node nodename -image target_image -isdefault true`
8. Verify that the target ONTAP software image is set as the default image for the node that you are reverting: `system image show`

The following example shows that version 9.1 is set as the default image on node0:

```

cluster1::*> system image show
          Is      Is
          Default Current Version      Install
Node     Image
----- ----- ----- -----
node0
        image1  false  true    9.2      MM/DD/YYYY TIME
        image2  true   false   9.1      MM/DD/YYYY TIME
node1
        image1  true   true    9.2      MM/DD/YYYY TIME
        image2  false  false   9.1      MM/DD/YYYY TIME
4 entries were displayed.

```

9. If the cluster consists of only two nodes, verify that the node does not hold epsilon:

a. Check whether the node currently holds epsilon: `cluster show -node nodename`

The following example shows that the node holds epsilon:

```
cluster1::*> cluster show -node node1

    Node: node1
    UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
    Epsilon: true
    Eligibility: true
    Health: true
```

b. If the node holds epsilon, mark epsilon as false on the node so that epsilon can be transferred to the node's partner: `cluster modify -node nodenameA -epsilon false`

c. Transfer epsilon to the node's partner by marking epsilon true on the partner node: `cluster modify -node nodenameB -epsilon true`

10. Verify that the node is ready for reversion: `system node revert-to -node nodename -check-only true -version 9.x`

The check-only parameter identifies any preconditions that must be addressed before reverting, such as the following examples:

- Disabling storage failover
- Disabling the Snapshot policy
- Deleting Snapshot copies that were created after upgrading to the later version of ONTAP

11. Verify that all of the preconditions have been addressed: `system node revert-to -node nodename -check-only true -version 9.x`

12. Revert the cluster configuration of the node: `system node revert-to -node nodename -version 9.x`

The -version option refers to the target release. For example, if the software you installed and verified is ONTAP 9.1, the correct value of the -version option is 9.1.

The cluster configuration is reverted, and then you are logged out of the clustershell.

13. Log back in to the clustershell, and then switch to the nodeshell: `run -node nodename`

After logging on the clustershell again, it might take a few minutes before it is ready to accept the nodeshell command. So, if the command fails, wait a few minutes and try it again.

14. Revert the file system configuration of the node: `revert_to 9.x`

This command verifies that the node's file system configuration is ready to be reverted, and then reverts it. If any preconditions are identified, you must address them and then rerun the `revert_to` command.



Using a system console to monitor the revert process displays greater details than seen in nodeshell.

When the command finishes, the LOADER prompt is displayed.

15. Enter `yes` at prompt to revert.

If AUTOBOOT is true, the node will reboot to ONTAP. If AUTOBOOT is false, the node will halt.

16. After the node has rebooted, confirm that the new software is running: `system node image show`

In the following example, image1 is the new ONTAP version and is set as the current version on node0:

```
cluster1::>*> system node image show
              Is      Is
              Node    Image  Default Current Version   Install
                                         Date
-----
node0
        image1  true    true     X.X.X      MM/DD/YYYY TIME
        image2  false   false     Y.Y.Y      MM/DD/YYYY TIME
node1
        image1  true    false    X.X.X      MM/DD/YYYY TIME
        image2  false   true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.
```

17. Verify that the revert status is complete for each node: `system node upgrade-revert show -node nodename`

The status should be listed as complete.

If the revert is not successful, contact technical support immediately.

18. Repeat [step-5] through [step-17] on the other node in the HA pair.
19. If the cluster consists of only two nodes, reenable cluster HA: `cluster ha modify -configured true`
20. Reenable storage failover on both nodes if it was previously disabled: `storage failover modify -node nodename -enabled true`
21. Repeat [step-6] through [step-18] for each additional HA pair and both the clusters in MetroCluster Configuration.

Things to verify after revert

After you revert, there are various tasks you need to perform to verify that your cluster is ready.

Verify cluster and storage health after downgrade or revert

After you downgrade or revert a cluster, you should verify that the nodes are healthy and eligible to participate in the cluster, and that the cluster is in quorum. You should also verify the status of your disks, aggregates, and volumes.

Verify cluster health

1. Verify that the nodes in the cluster are online and are eligible to participate in the cluster: `cluster show`

```
cluster1::> cluster show
Node          Health  Eligibility
-----
node0        true    true
node1        true    true
```

If any node is unhealthy or ineligible, check EMS logs for errors and take corrective action.

2. Set the privilege level to advanced: `set -privilege advanced`
3. Enter `y` to continue.
4. Verify the configuration details for each RDB process.

- The relational database epoch and database epochs should match for each node.
- The per-ring quorum master should be the same for all nodes.

Note that each ring might have a different quorum master.

To display this RDB process...	Enter this command...
Management application	<code>cluster ring show -unitname mgmt</code>
Volume location database	<code>cluster ring show -unitname vldb</code>
Virtual-Interface manager	<code>cluster ring show -unitname vifmgr</code>
SAN management daemon	<code>cluster ring show -unitname bcomd</code>

This example shows the volume location database process:

```

cluster1::>* cluster ring show -unitname vldb
Node      UnitName Epoch     DB Epoch DB Trnxs Master     Online
-----  -----  -----  -----  -----  -----  -----
node0      vldb      154      154      14847    node0      master
node1      vldb      154      154      14847    node0      secondary
node2      vldb      154      154      14847    node0      secondary
node3      vldb      154      154      14847    node0      secondary
4 entries were displayed.

```

1. If you are operating in a SAN environment, verify that each node is in a SAN quorum: `event log show -messagename scsiblade.*`

The most recent scsiblade event message for each node should indicate that the scsi-blade is in quorum.

```

cluster1::>* event log show -messagename scsiblade.*
Time          Node          Severity      Event
-----  -----
-----  -----
MM/DD/YYYY TIME  node0          INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1          INFORMATIONAL scsiblade.in.quorum: The
scsi-blade ...

```

2. Return to the admin privilege level: `set -privilege admin`

Related information

[System administration](#)

[Verify storage health](#)

After you revert or downgrade a cluster, you should verify the status of your disks, aggregates, and volumes.

1. Verify disk status:

To check for...	Do this...
Broken disks	<ul style="list-style-type: none"> a. Display any broken disks: <code>storage disk show -state broken</code> b. Remove or replace any broken disks.

To check for...	Do this...
Disks undergoing maintenance or reconstruction	<p>a. Display any disks in maintenance, pending, or reconstructing states: <code>storage disk show -state maintenance pending reconstructing</code></p> <p>b. Wait for the maintenance or reconstruction operation to finish before proceeding.</p>

2. Verify that all aggregates are online by displaying the state of physical and logical storage, including storage aggregates: `storage aggregate show -state !online`

This command displays the aggregates that are *not* online. All aggregates must be online before and after performing a major upgrade or reversion.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verify that all volumes are online by displaying any volumes that are *not* online: `volume show -state !online`

All volumes must be online before and after performing a major upgrade or reversion.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Verify that there are no inconsistent volumes: `volume show -is-inconsistent true`

If any inconsistent volumes are returned, you must contact NetApp Support before you proceed with the upgrade.

Related information

Disk and aggregate management

Enable automatic switchover for MetroCluster configurations

This topic provides information regarding the additional tasks that you must perform after the reversion of MetroCluster configurations.

1. Enable automatic unplanned switchover: `metrocluster modify -auto-switchover-failure -domain auso-on-cluster-disaster`
2. Validate the MetroCluster configuration: `metrocluster check run`

Enable and revert LIFs to home ports after a revert

During a reboot, some LIFs might have been migrated to their assigned failover ports. After you revert a cluster, you must enable and revert any LIFs that are not on their home ports.

The network interface revert command reverts a LIF that is not currently on its home port back to its home port, provided that the home port is operational. A LIF's home port is specified when the LIF is created; you can determine the home port for a LIF by using the network interface show command.

1. Display the status of all LIFs: `network interface show`

This example displays the status of all LIFs for a storage virtual machine (SVM).

```
cluster1::> network interface show -vserver vs0
      Logical     Status      Network          Current
Current Is
Vserver      Interface   Admin/Oper Address/Mask      Node      Port
Home
-----
-----
vs0
      true       data001    down/down  192.0.2.120/24    node0    e0e
      true       data002    down/down  192.0.2.121/24    node0    e0f
      true       data003    down/down  192.0.2.122/24    node0    e2a
      true       data004    down/down  192.0.2.123/24    node0    e2b
      false      data005    down/down  192.0.2.124/24    node0    e0e
      false      data006    down/down  192.0.2.125/24    node0    e0f
      false      data007    down/down  192.0.2.126/24    node0    e2a
      false      data008    down/down  192.0.2.127/24    node0    e2b
8 entries were displayed.
```

If any LIFs appear with a Status Admin status of down or with an Is home status of false, continue with the next step.

2. Enable the data LIFs: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up  
8 entries were modified.
```

3. Revert LIFs to their home ports: `network interface revert *`

This command reverts all LIFs back to their home ports.

```
cluster1::> network interface revert *\n8 entries were acted on.
```

4. Verify that all LIFs are in their home ports: `network interface show`

This example shows that all LIFs for SVM vs0 are on their home ports.

```
cluster1::> network interface show -vserver vs0\n      Logical     Status      Network          Current\nCurrent Is\nVserver    Interface Admin/Oper Address/Mask      Node       Port\nHome\n-----\n-----\nvs0\n      data001    up/up     192.0.2.120/24    node0     e0e\ntrue\n      data002    up/up     192.0.2.121/24    node0     e0f\ntrue\n      data003    up/up     192.0.2.122/24    node0     e2a\ntrue\n      data004    up/up     192.0.2.123/24    node0     e2b\ntrue\n      data005    up/up     192.0.2.124/24    node1     e0e\ntrue\n      data006    up/up     192.0.2.125/24    node1     e0f\ntrue\n      data007    up/up     192.0.2.126/24    node1     e2a\ntrue\n      data008    up/up     192.0.2.127/24    node1     e2b\n8 entries were displayed.
```

Enable Snapshot copy policies after reverting

After reverting to an earlier version of ONTAP, you must enable Snapshot copy policies to

start creating Snapshot copies again.

You are reenabling the Snapshot schedules that you disabled before you reverted to an earlier version of ONTAP.

1. Enable Snapshot copy policies for all data SVMs:

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. For each node, enable the Snapshot copy policy of the root volume by using the run-node nodenamevol optionsroot_vol_namenosnap off command.

```
cluster1::> run -node node1 vol options vol0 nosnap off
```

Verify client access (CIFS and NFS)

For the configured protocols, test access from CIFS and NFS clients to verify that the cluster is accessible.

Verify IPv6 firewall entries

A reversion from any version of ONTAP 9 might result in missing default IPv6 firewall entries for some services in firewall policies. You need to verify that the required firewall entries have been restored to your system.

1. Verify that all firewall policies are correct by comparing them to the default policies: `system services firewall policy show`

The following example shows the default policies:

```

cluster1::*> system services firewall policy show
Policy          Service      Action IP-List
-----
cluster
        dns      allow  0.0.0.0/0
        http     allow  0.0.0.0/0
        https    allow  0.0.0.0/0
        ndmp     allow  0.0.0.0/0
        ntp      allow  0.0.0.0/0
        rsh      allow  0.0.0.0/0
        snmp    allow  0.0.0.0/0
        ssh      allow  0.0.0.0/0
        telnet   allow  0.0.0.0/0
data
        dns      allow  0.0.0.0/0, ::/0
        http     deny   0.0.0.0/0, ::/0
        https    deny   0.0.0.0/0, ::/0
        ndmp     allow  0.0.0.0/0, ::/0
        ntp      deny   0.0.0.0/0, ::/0
        rsh      deny   0.0.0.0/0, ::/0
.
.
.

```

2. Manually add any missing default IPv6 firewall entries by creating a new firewall policy: `system services firewall policy create`

```

cluster1::*> system services firewall policy create -policy newIPv6
-service ssh -action allow -ip-list ::/0

```

3. Apply the new policy to the LIF to allow access to a network service: `network interface modify`

```

cluster1::*> network interface modify -vserver VS1 -lif LIF1
-firewall-policy newIPv6

```

Revert password hash function to the supported encryption type

If you revert to a release prior from any version of ONTAP 9, SHA-2 account users can no longer be authenticated with their passwords. Therefore, you must have them reset their passwords to using the encryption type (MD5) that is supported by the release you revert to.

- Prior to the revert, identify the user accounts that use the SHA-2 hash function (advanced privilege level):

```
security login show -vserver * -username * -application * -authentication  
-method password -hash-function !md5
```

You should retain the command output. You need the account information after the revert.

- During the revert, run the advanced command security Login password-prepare-to-downgrade as prompted to reset your own password to using the MD5 hash function.

If your password is not encrypted with MD5, the command prompts you for a new password and encrypts it with MD5, enabling your credential to be authenticated after the revert.

- After the revert, reset SHA-2 accounts to MD5:

- For each SHA-2 account you identified, change the password to a temporary one: `security login password -username user_name -vserver vserver_name`

The changed password uses the MD5 hash function.

- Communicate the temporary password to the affected users and have them log in through a console or SSH session to change their passwords as prompted by the system.

Considerations for whether to manually update the SP firmware

If the SP automatic update functionality is enabled (the default), downgrading or reverting to ONTAP 8.3.x does not require a manual SP firmware update. The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to.

If the SP automatic update functionality is disabled (not recommended), after the ONTAP revert or downgrade process is complete, you must manually update the SP firmware to a version that is supported for the ONTAP version you reverted or downgraded to.

[NetApp BIOS/ONTAP Support Matrix](#)

[NetApp Downloads: System Firmware and Diagnostics](#)

ONTAP 9 Network Management Documentation

ONTAP System Manager enables rich networking visualization and the ability to download consolidated data about your network. You can learn more in the following topics:

- [View and manage your network](#)
- [Download network data for reporting](#)

You can also set up and manage your network with the ONTAP CLI. The ONTAP 9 CLI network management documentation consists of three main areas:

[Set up NAS path failover for ONTAP 9.8 and later](#)

Learn how to set up NAS path failover using established best practices in ONTAP 9.8 and later

[Set up NAS path failover for ONTAP 9.7 and earlier](#)

Learn how to set up NAS path failover using established best practices in ONTAP 9.7 and earlier.

[Networking reference](#)

The networking reference documentation describes how to configure and manage physical and virtual network ports (VLANs and interface groups), LIFs using IPv4 and IPv6, routing, and host-resolution services in clusters; optimize network traffic by load balancing; and monitor the cluster by using SNMP. Unless otherwise stated, this content applies to all versions of ONTAP 9.

Viewing and managing your network

Starting with System Manager 9.8, you can display a graphic that shows the components and configuration of your network.

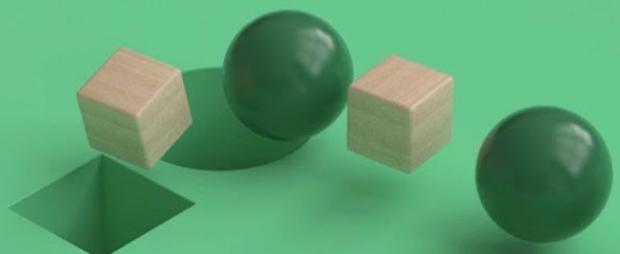
The new network visualization feature enables users to see the network connections path across hosts, ports, SVMs, volumes, etc. in a graphical interface.

ONTAP System Manager 9.8

Network Visualization

Tech Clip

 NetApp



The graphic displays when you select **Network > Overview** or when you select → from the **Network** section of the Dashboard.

The following categories of components are shown in the graphic:

- Hosts
- Storage ports
- Network interfaces
- Storage VMs
- Data access components

Each section shows additional details that you can hover your mouse over or select to perform network management and configuration tasks.

Examples

The following are some examples of the many ways you can interact with the graphic to view details about each component or initiate actions to manage your network:

- Click on a host to see its configuration: the ports, network interfaces, storage VMs, and data access components associated with it.
- Hover the mouse over the number of volumes in a storage VM to select a volume to view its details.
- Select an iSCSI interface to view its performance over the last week.
- Click on : next to a component to initiate actions to modify that component.
- Quickly determine where problems might occur in your network, indicated by an "X" next to unhealthy components.

Downloading network data for reporting

Starting with System Manager 9.8, you can download the data that is displayed in System Manager about your network.

When you display information in a *List View*, you can click **Download**, and the list of objects displayed is downloaded.

- The list is downloaded in comma-separated values (CSV) format.
- Only the data in the visible columns is downloaded.
- The CSV filename is formatted with the object name and a time stamp.

Set up NAS path failover (ONTAP 9.8 and later CLI)

This workflow guides you through the networking configuration steps to set up NAS path failover for ONTAP 9.8 and later. This workflow assumes the following:

- You want to use NAS path failover best practices in a workflow that simplifies network configuration.
- You want to use the CLI, not ONTAP System Manager.
- You are configuring networking on a new system running ONTAP 9.8 or later.

If you are running an ONTAP release earlier than 9.8, you should use the following NAS path failover procedure for ONTAP 9.0 to 9.7:

- [ONTAP 9.0 - 9.7 NAS Path Failover Workflow](#)

If you want network management details, you should use the following ONTAP 9 Network Management Reference:

- [ONTAP 9 Network Management Reference](#)

If you want to use ONTAP System Manager to configure the network for ONTAP 9.7 and later, you should choose the following documentation:

- [ONTAP System Manager docs](#)

If you want to use OnCommand System Manager to configure the network for ONTAP 9.7 and earlier, you should choose the following documentation:

- [Cluster management using System Manager](#)

If you require additional configuration or conceptual information, you should choose among the following documentation:

- Conceptual background for network configuration
 - [ONTAP concepts](#)
- NAS file access
 - [NFS management](#)
 - [SMB/CIFS management](#)

- SAN host provisioning
 - [SAN administration](#)
- Command reference
 - [ONTAP 9 commands](#)
- Technical Reports (TRs), which include additional information about ONTAP technology and interaction with external services
 - [NetApp Technical Report 4182: Ethernet Storage Design Considerations and Best Practices for Clustered Data ONTAP Configurations](#)

Workflow NAS path failover

Overview

If you are already familiar with basic networking concepts, you might be able to save time setting up your network by reviewing this "hands on" workflow for NAS path failover configuration.

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. You can rely on the ONTAP defaults to manage path failover.



A SAN LIF does not migrate (unless you move it manually after the link failure). Instead, multipathing technology on the host diverts traffic to a different LIF. For more information, see [SAN administration](#).

Worksheet for NAS path failover configuration for ONTAP 9.8 and later

You should complete all sections of the worksheet before configuring NAS path failover.

IPspace configuration

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Information	Required?	Your values
IPspace name The unique identifier of the IPspace.	Yes	

Broadcast domain configuration

A broadcast domain groups ports that belong in the same Layer 2 network and sets the MTU for the broadcast domain ports.

Broadcast domains are assigned to an IPspace. An IPspace can contain one or more broadcast domains.



The port to which a LIF fails over must be a member of the failover group for the LIF. For each broadcast domain created by ONTAP, a failover group with the same name is also created that contains all the ports in the broadcast domain.

Information	Required?	Your values
IPspace name The IPspace to which the broadcast domain is assigned. This IPspace must exist.	Yes	
Broadcast domain name The name of the broadcast domain. This name must be unique in the IPspace.	Yes	
MTU The maximum transmission unit value for the broadcast domain, either 1500 or 9000 . The MTU value is applied to all ports in the broadcast domain and to any ports that are later added to the broadcast domain. The MTU value must match all the devices connected to that network except for e0M port handling management traffic.	Yes	
Ports Ports are assigned to broadcast domains based on reachability. After port assignment is complete, check reachability by running the <code>network port reachability show</code> command. These ports can be physical ports, VLANs, or interface groups.	Yes	

Subnet configuration

A subnet contains pools of IP addresses and a default gateway that can be assigned to LIFs used by SVMs residing in the IPspace.

- When creating a LIF on an SVM, you can specify the name of the subnet instead of supplying an IP address and a subnet.
- Since a subnet can be configured with a default gateway, you do not have to create the default gateway in a separate step when creating an SVM.
- A broadcast domain can contain one or more subnets.
- You can configure SVM LIFs that are on different subnets by associating more than one subnet with the IPspace's broadcast domain.
- Each subnet must contain IP addresses that do not overlap with IP addresses assigned to other subnets in the same IPspace.
- You can assign specific IP addresses to SVM data LIFs and create a default gateway for the SVM instead of using a subnet.

Information	Required?	Your values
IPspace name The IPspace to which the subnet will be assigned. This IPspace must exist.	Yes	
Subnet name The name of the subnet. This name must be unique in the IPspace.	Yes	
Broadcast domain name The broadcast domain to which the subnet will be assigned. This broadcast domain must reside in the specified IPspace.	Yes	
Subnet name and mask The subnet and mask in which the IP addresses reside.	Yes	
Gateway You can specify a default gateway for the subnet. If you do not assign a gateway when you create the subnet, you can assign one later.	No	

Information	Required?	Your values
<p>IP address ranges You can specify a range of IP addresses or specific IP addresses.</p> <p>For example, you can specify a range such as:</p> <pre>192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145</pre> <p>If you do not specify an IP address range, the entire range of IP addresses in the specified subnet are available to assign to LIFs.</p>	No	
<p>Force update of LIF associations Specifies whether to force the update of existing LIF associations.</p> <p>By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided.</p> <p>Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed.</p>	No	

SVM configuration

You use SVMs to serve data to clients and hosts.

The values you record are for creating a default data SVM. If you are creating a MetroCluster source SVM, see the [Fabric-attached MetroCluster Installation and Configuration Guide](#) or the [Stretch MetroCluster Installation and Configuration Guide](#).

Information	Required?	Your values
<p>SVM name The fully qualified domain name (FQDN) of the SVM.</p> <p>This name must be unique across cluster leagues.</p>	Yes	
<p>Root volume name The name of the SVM root volume.</p>	Yes	

Information	Required?	Your values
Aggregate name The name of the aggregate that holds the SVM root volume. This aggregate must exist.	Yes	
Security style The security style for the SVM root volume. Possible values are ntfs , unix , and mixed .	Yes	
IPspace name The IPSpace to which the SVM is assigned. This IPSpace must exist.	No	
SVM language setting The default language to use for the SVM and its volumes. If you do not specify a default language, the default SVM language is set to C.UTF-8 . The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM. You can modify The language after the SVM is created.	No	

LIF configuration

An SVM serves data to clients and hosts through one or more network logical interfaces (LIFs).

Information	Required?	Your values
SVM name The name of the SVM for the LIF.	Yes	

Information	Required?	Your values
<p>LIF name The name of the LIF.</p> <p>You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports.</p> <p>To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes.</p> <p>Important: If you are configuring a SMB server to host Hyper-V or SQL Server over SMB for nondisruptive operation solutions, the SVM must have at least one data LIF on every node in the cluster.</p>	Yes	
<p>Service policy Service policy for the LIF.</p> <p>The service policy defines which network services can use the LIF. Built-in services and service policies are available for managing data and management traffic on both data and system SVMs.</p>	Yes	
<p>Allowed protocols IP-based LIFs do not require allowed protocols, use the service policy row instead.</p> <p>Specify allowed protocols for SAN LIFs on FibreChannel ports. These are the protocols that can use that LIF. The protocols that use the LIF cannot be modified after the LIF is created. You should specify all protocols when you configure the LIF.</p>	No	

Information	Required?	Your values
<p>Home node The node to which the LIF returns when the LIF is reverted to its home port.</p> <p>You should record a home node for each data LIF.</p>	Yes	
<p>Home port or broadcast domain Chose one of the following:</p> <p>Port: Specify the port to which the logical interface returns when the LIF is reverted to its home port. This is only done for the first LIF in the subnet of an IPspace, otherwise it is not required.</p> <p>Broadcast Domain: Specify the broadcast domain, and the system will select the appropriate port to which the logical interface returns when the LIF is reverted to its home port.</p>	Yes	
<p>Subnet name The subnet to assign to the SVM.</p> <p>All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet.</p>	Yes (if using a subnet)	

DNS configuration

You must configure DNS on the SVM before creating an NFS or SMB server.

Information	Required?	Your values
<p>SVM name The name of the SVM on which you want to create an NFS or SMB server.</p>	Yes	
<p>DNS domain name A list of domain names to append to a host name when performing host- to-IP name resolution.</p> <p>List the local domain first, followed by the domain names for which DNS queries are most often made.</p>	Yes	

Information	Required?	Your values
<p>IP addresses of the DNS servers List of IP addresses for the DNS servers that will provide name resolution for the NFS or SMB server.</p> <p>The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the SMB server will join.</p> <p>The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. SMB server creation fails if ONTAP cannot obtain the service location records through local DNS queries.</p> <p>The simplest way to ensure that ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers.</p> <p>You can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers.</p> <p>For information about the Active Directory-integrated SRV records, see the topic How DNS Support for Active Directory Works on Microsoft TechNet.</p>	Yes	

Dynamic DNS configuration

Before you can use dynamic DNS to automatically add DNS entries to your Active Directory- integrated DNS servers, you must configure dynamic DNS (DDNS) on the SVM.

DNS records are created for every data LIF on the SVM. By creating multiple data LIFS on the SVM, you can load-balance client connections to the assigned data IP addresses. DNS load balances connections that are made using the host name to the assigned IP addresses in a round- robin fashion.

Information	Required?	Your values
SVM name The SVM on which you want to create an NFS or SMB server.	Yes	
Whether to use DDNS Specifies whether to use DDNS. The DNS servers configured on the SVM must support DDNS. By default, DDNS is disabled.	Yes	
Whether to use secure DDNS Secure DDNS is supported only with Active Directory-integrated DNS. If your Active Directory-integrated DNS allows only secure DDNS updates, the value for this parameter must be true. By default, secure DDNS is disabled. Secure DDNS can be enabled only after a SMB server or an Active Directory account has been created for the SVM.	No	
FQDN of the DNS domain The FQDN of the DNS domain. You must use the same domain name configured for DNS name services on the SVM.	No	

Create IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Before you begin

You must be a cluster administrator to perform this task.

Step

Create an IPspace.

```
network ipspace create -ipspace ipspace1
```

```
network ipspace show
```

IPspace	Vserver List	Broadcast Domains
Cluster	Cluster	Cluster
Default	Cluster1	Default
ipspace1	ipspace1	-

The IPspace is created, along with the system SVM for the IPspace. The system SVM carries management traffic.

Move broadcast domains into IPspaces

Move the broadcast domains that the system created based on layer 2 reachability into the IPspaces you created.

Before you move the broadcast domain, you must verify the reachability of the ports in your broadcast domains.

The automatic scanning of ports can determine which ports can reach each other and place them in the same broadcast domain, but this scanning is unable to determine the appropriate IPspace. If the broadcast domain belongs in a non-default IPspace, then you must move it manually using the steps in this section.

Before you begin

Broadcast domains are automatically configured as part of cluster create and join operations. ONTAP defines the "Default" broadcast domain to be the set of ports that have layer 2 connectivity to the home port of the management interface on the first node created in the cluster. Other broadcast domains are created, if necessary, and are named **Default-1**, **Default-2**, and so forth.

When a node joins an existing cluster, their network ports automatically join existing broadcast domains based on their layer 2 reachability. If they do not have reachability to an existing broadcast domain, the ports are placed into one or more new broadcast domains.

About this task

- Ports with cluster LIFs are automatically placed into the "Cluster" IPspace.
- Ports with reachability to the home port of the node-management LIF are placed into the "Default" broadcast domain.
- Other broadcast domains are created by ONTAP automatically as part of the cluster create or join operation.
- As you add VLANs and interface groups, they are automatically placed into the appropriate broadcast domain about a minute after they are created.

Steps

1. Verify the reachability of the ports in your broadcast domains. ONTAP automatically monitors layer 2 reachability. Use the following command to verify each port has been added to a broadcast domain and has "ok" reachability.

```
network port reachability show -detail
```

2. If necessary, move broadcast domains into other IPspaces:

```
network port broadcast-domain move
```

For example, if you want to move a broadcast domain from "Default" to "ips1":

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default  
-to-ipspace ips1
```

Repair port reachability

Broadcast domains are automatically created. However, if a port is recabled, or the switch configuration changes, a port might need to be repaired into a different broadcast domain (new or existing).

Before you begin

You must be a cluster administrator to perform this task.

About this task

A command is available to automatically repair the broadcast domain configuration for a port based on the layer 2 reachability detected by ONTAP.

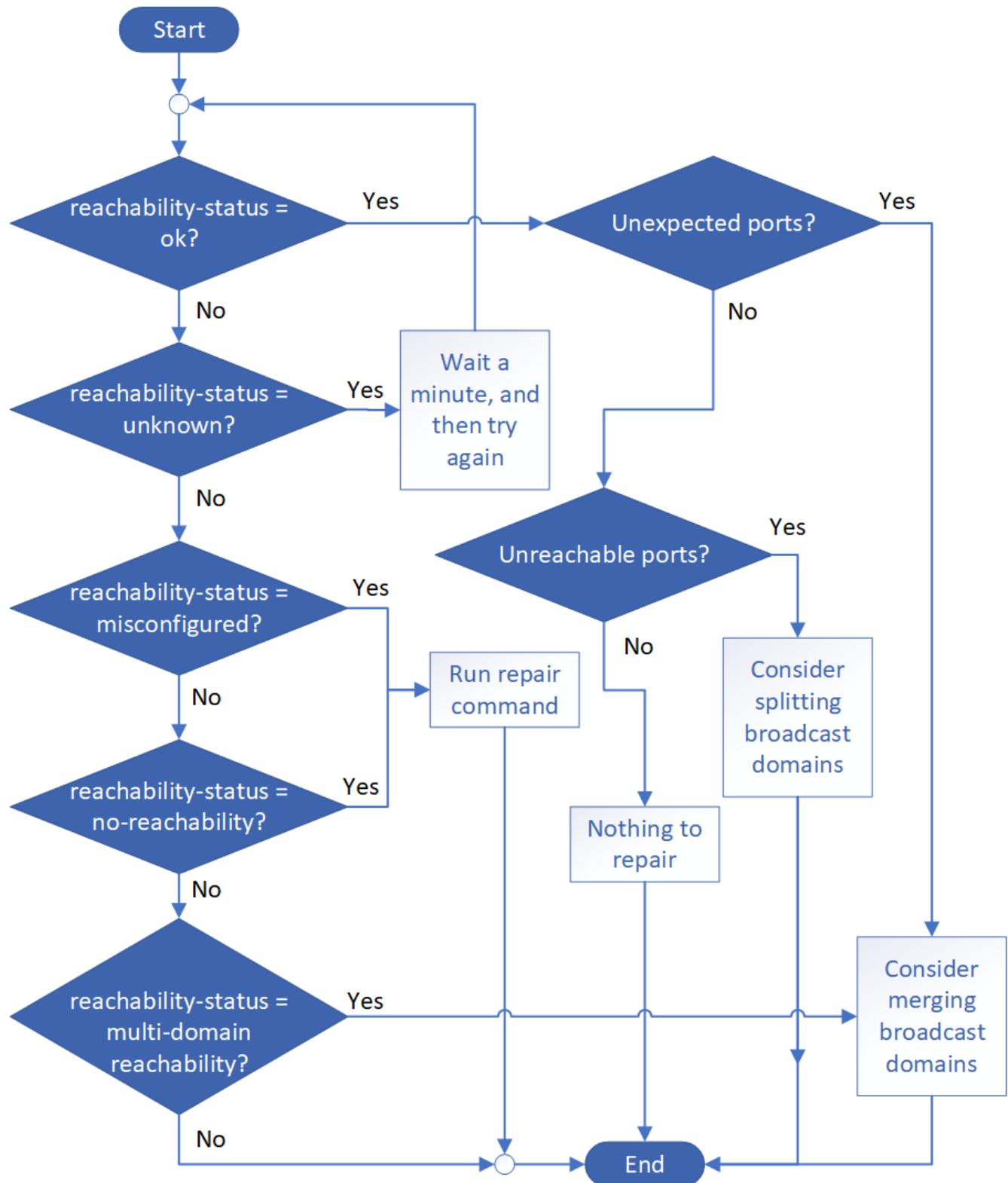
Steps

1. Check your switch configuration and cabling.
2. Check the reachability of the port:

```
network port reachability show -detail -node -port
```

The command output contains reachability results.

3. Use the following decision tree and table to understand the reachability results and determine what, if anything, to do next.



Reachability-status	Description
ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see the following <i>Unexpected ports</i> row.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see the following <i>Unreachable ports</i> row.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
Unexpected ports	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see Merge broadcast domains.</p>
Unreachable ports	<p>If a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology.</p> <p>Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain after you have verified that the physical and switch configuration is accurate.</p> <p>For more information, see Split broadcast domains.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre>network port reachability repair -node -port</pre>

Reachability-status	Description
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre data-bbox="820 439 1498 502">network port reachability repair -node -port</pre>
multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see Merge broadcast domains.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

After you repair a port, check for displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group.

LIFs

When a port is repaired and moved into a different broadcast domain, any LIFs that were configured on the repaired port will be automatically assigned a new home port. That home port is selected from the same broadcast domain on the same node, if possible. Alternatively, a home port from another node is selected, or, if no suitable home ports exist, the home port will be cleared.

If a LIF's home port is moved to another node, or is cleared, then the LIF is considered to have been "displaced". You can view these displaced LIFs with the following command:

```
displaced-interface show
```

If there are any displaced LIFs, you must either:

- Restore the home of the displaced LIF:

```
displaced-interface restore
```

- Set the home of the LIF manually:

```
network interface modify -home-port -home-node
```

- Remove the entry from the "displaced-interface" table if you are satisfied with the LIF's currently configured

home:

```
displaced-interface delete
```

VLANs

If the repaired port had VLANs, those VLANs are automatically deleted but are also recorded as having been "displaced". You can view these displaced VLANs:

```
displaced-vlans show
```

If there are any displaced VLANs, you must either:

- Restore the VLANs to another port:

```
displaced-vlans restore
```

- Remove the entry from the "displaced-vlans" table:

```
displaced-vlans delete
```

Interface groups

If the repaired port was part of an interface group, it is removed from that interface group. If it was the only member port assigned to the interface group, the interface group itself is removed.

Related topics

[Verify your network configuration after upgrading](#)

[Monitor the reachability of network ports](#)

Create SVMs

You must create an SVM to serve data to clients.

Before you begin

- You must be a cluster administrator to perform this task.
- You must know which security style the SVM root volume will have.

If you plan to implement a Hyper-V or SQL Server over SMB solution on this SVM, you should use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style data volumes.

Steps

1. Determine which aggregates are candidates for containing the SVM root volume.

```
storage aggregate show -has-mroot false
```

You must choose an aggregate that has at least 1 GB of free space to contain the root volume. If you intend to configure NAS auditing on the SVM, you must have a minimum of 3 GB of extra free space on the

root aggregate, with the extra space being used to create the auditing staging volume when auditing is enabled.



If NAS auditing is already enabled on an existing SVM, the aggregate's staging volume is created immediately after aggregate creation is successfully completed.

2. Record the name of the aggregate on which you want to create the SVM root volume.
3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:

```
vserver create -language ?
```

4. If you plan on specifying a Snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the Snapshot policy you want to use:

```
volume snapshot policy show -vserver <vserver_name>
```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume quota policy show -vserver <vserver_name>
```

6. Create an SVM:

```
vserver create -vserver <vserver_name> -aggregate <aggregate_name> -rootvolume <root_volume_name> -rootvolume-security-style {unix|ntfs|mixed} [-ipspace <IPspace_name>] [-language <language>] [-snapshot-policy <snapshot_policy_name>] [-quota-policy <quota_policy_name>] [-comment <comment>]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root -rootvolume-security-style ntfs -ipspace ipspace1 -language en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. Verify that the SVM configuration is correct.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowered Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In this example, the command creates the SVM named "vs1" in IPspace "ipspace1". The root volume is named "vs1_root" and is created on aggr3 with NTFS security style.

Create LIFs

An SVM serves data to clients through one or more network logical interfaces (LIFs). You must create LIFs on the ports you want to use to access data.

Before you begin

You must be a cluster administrator to perform this task.

About this task

Starting with ONTAP 9.7, ONTAP automatically chooses the home port of a LIF, as long as at least one LIF already exists in the same subnet in that IPspace. ONTAP chooses a home-port in the same broadcast domain as other LIFs in that subnet. You can still specify a home port, but it is no longer required (unless no LIFs yet exist in that subnet in the specified IPspace).

You should not configure LIFs that carry CIFS traffic to automatically revert to their home nodes. This recommendation is mandatory if the CIFS server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.

Steps

1. Determine which broadcast domain ports you want to use for the LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

IPspace	Broadcast	MTU	Port List	Update Status	Details
Name	Domain name				
ipspace1	default	1500			
			node1:e0d	complete	
			node1:e0e	complete	
			node2:e0d	complete	
			node2:e0e	complete	

2. Verify that the subnet you want to use for the LIFs contains sufficient unused IP addresses.

```
network subnet show -ipspace ipspace1
```

3. Create one or more LIFs on the ports you want to use to access data.

```
network interface create -vserver vs1 -lif lif1 -home-node node1 -home-port e0d -service-policy default-data-files -subnet-name ipspace1
```

4. Verify that the LIF interface configuration is correct.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
vs1						
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	true

5. Verify that the failover group configuration is as desired.

```
network interface show -failover -vserver vs1
```

Vserver	Logical interface	Home Node:Port	Failover Policy	Failover Group
vs1	lif1	node1:e0d	system-defined	ipspace1
		Failover Targets:	node1:e0d, node1:e0e, node2:e0d, node2:e0e	

Configure DNS services

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are files and dns.

You must ensure that dns is one of the sources before you create the SMB server.



To view the statistics for DNS name services for the mgwd process and SecD process, use the Statistics UI.

Steps

1. Determine what the current configuration is for the hosts name services database. In this example, the hosts name service database uses the default settings.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Perform the following actions, if required.

- a. Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

In this example, the hosts database is configured to use DNS and local files in that order.

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

- b. Verify that the name services configuration is correct.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. Configure DNS services.

```
vserver services name-service dns create -vserver vs1 -domains example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```



The vserver services name-service dns create command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

4. Verify that the DNS configuration is correct and that the service is enabled.

```
Vserver: vs1  
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51  
Enable/Disable DNS: enabled Timeout (secs): 2  
Maximum Attempts: 1
```

5. Validate the status of the name servers.

```
vserver services name-service dns check -vserver vs1
```

Vserver	Name Server	Status	Status Details
vs1	10.0.0.50	up	Response time (msec): 2
vs1	10.0.0.51	up	Response time (msec): 2

Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified fully qualified domain name (FQDN) must be unique:

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB/CIFS, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

          Vserver: vs1
          CIFS Server NetBIOS Name: CIFS_VS1
          NetBIOS Domain/Workgroup Name: EXAMPLE
          Fully Qualified Domain Name: EXAMPLE.COM
          Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
          Workgroup Name: -
          Kerberos Realm: -
          Authentication Style: domain
CIFS Server Administrative Status: up
          CIFS Server Description:
          List of NetBIOS Aliases: -
```



To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see [RFC 1123](#).

Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false}] -vserver-fqdn
FQDN_used_for_DNS_updates
```

```
vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, `*.netapp.com` is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

Vserver	Is-Enabled	Use-Secure	Vserver FQDN	TTL
vs1	true	true	vs1.example.com	24h

Get more information

You can get help and find more information through various resources, documentation, and forums.

- [Documentation](#) – Release Notes and Guides for this release and previous releases.

- [NetApp TechCommTV](#) – NetApp videos.
- [NetApp resources](#) – Technical Reports and Knowledgebase Articles.
- [NetApp Community](#) – NetApp product and solutions forums.

Set up NAS path failover (ONTAP 9.0 - 9.7 CLI)

This workflow guides you through the networking configuration steps to set up NAS path failover for ONTAP 9.0 - 9.7. This workflow assumes the following:

- You want to use NAS path failover best practices that simplify network configuration.
- You want to use the CLI, not ONTAP System Manager.
- You are configuring networking on a new system running ONTAP 9.0 to 9.7.

If you are running an ONTAP release later than 9.7, you should use the NAS path failover procedure for ONTAP 9.8 or later:

- [ONTAP 9.8 and later NAS Path Failover Workflow](#)

If you want network management details, you should use the following ONTAP 9 Network Management Reference:

- [ONTAP 9 Network Management Reference](#)

If you want to use ONTAP System Manager to configure the network for ONTAP 9.7 and later, you should choose the following documentation:

- [ONTAP System Manager docs](#)

If you want to use OnCommand System Manager to configure the network for ONTAP 9.7 and earlier, you should choose the following documentation:

- [Cluster management using System Manager](#)

If you require additional configuration or conceptual information, you should choose among the following documentation:

- Conceptual background for network configuration
 - [ONTAP concepts](#)
- NAS file access
 - [NFS management](#)
 - [SMB/CIFS management](#)
- SAN host provisioning
 - [SAN administration](#)
- Command reference
 - [ONTAP 9 commands](#)
- Technical Reports (TRs), which include additional information about ONTAP technology and interaction with external services

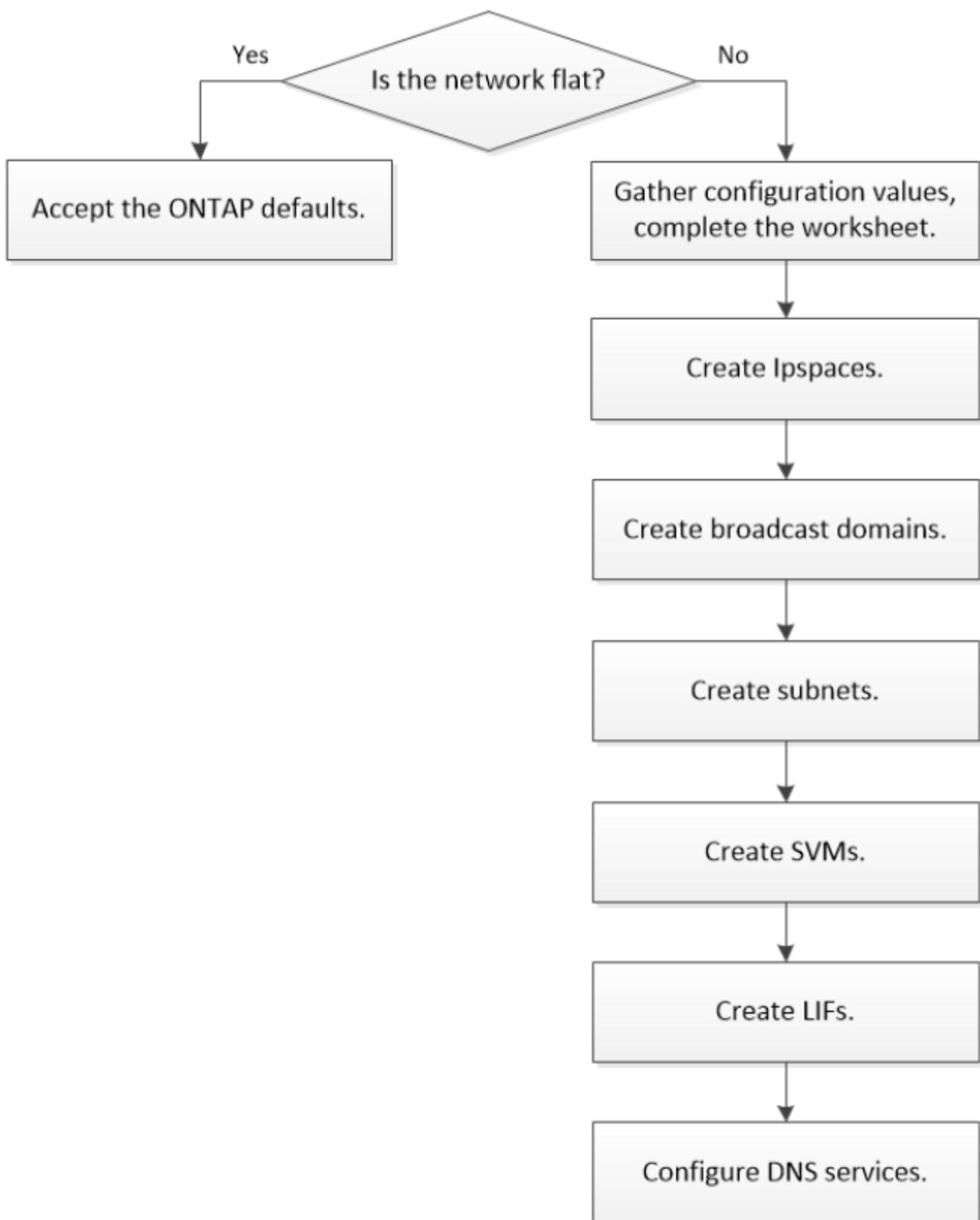
- NetApp Technical Report 4182: Ethernet Storage Design Considerations and Best Practices for Clustered Data ONTAP Configurations

Workflow NAS path failover

Overview

If you are already familiar with basic networking concepts, you might be able to save time setting up your network by reviewing this "hands on" workflow for NAS path failover configuration.

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. If your network is flat, you can rely on the ONTAP defaults to manage path failover. Otherwise, you should configure path failover following the steps in this workflow.



A SAN LIF does not migrate (unless you move it manually after the link failure). Instead, multipathing technology on the host diverts traffic to a different LIF. For more information, see [SAN administration](#).

Worksheet for NAS path failover configuration for ONTAP 9.0 - 9.7

You should complete all sections of the worksheet before configuring NAS path failover.

IPspace configuration

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Information	Required?	Your values
IPspace name <ul style="list-style-type: none">• The name of the IPspace.• The name must be unique in the cluster.	Yes	

Broadcast domain configuration

A broadcast domain groups ports that belong in the same Layer 2 network and sets the MTU for the broadcast domain ports.

Broadcast domains are assigned to an IPspace. An IPspace can contain one or more broadcast domains.



The port to which a LIF fails over must be a member of the failover group for the LIF. When you create a broadcast domain, ONTAP automatically creates a failover group with the same name. The failover group contains all the ports assigned to the broadcast domain.

Information	Required?	Your values
IPspace name <ul style="list-style-type: none">• The IPspace to which the broadcast domain is assigned.• The IPspace must exist.	Yes	
Broadcast domain name <ul style="list-style-type: none">• The name of the broadcast domain.• This name must be unique in the IPspace.	Yes	

Information	Required?	Your values
<p>MTU</p> <ul style="list-style-type: none"> The MTU of the broadcast domain. You can specify either 1500 or 9000. The MTU value is applied to all ports in the broadcast domain and to any ports that are later added to the broadcast domain. <p> The MTU value must match all the devices connected to that network except for e0M port handling management traffic.</p>	Yes	
<p>Ports</p> <ul style="list-style-type: none"> The network ports to add to the broadcast domain. The ports assigned to the broadcast domain can be physical ports, VLANs, or interface groups (ifgroups). If a port is in another broadcast domain, it must be removed before it can be added to the broadcast domain. Ports are assigned by specifying both the node name and port: for example, node1:e0d. 	Yes	

Subnet configuration

A subnet contains pools of IP addresses and a default gateway that can be assigned to LIFs used by SVMs residing in the IPspace.

- When creating a LIF on an SVM, you can specify the name of the subnet instead of supplying an IP address and a subnet.
- Since a subnet can be configured with a default gateway, you do not have to create the default gateway in a separate step when creating an SVM.

- A broadcast domain can contain one or more subnets.
You can configure SVM LIFs that are on different subnets by associating more than one subnet with the IPspace's broadcast domain.
- Each subnet must contain IP addresses that do not overlap with IP addresses assigned to other subnets in the same IPspace.
- You can assign specific IP addresses to SVM data LIFs and create a default gateway for the SVM instead of using a subnet.

Information	Required?	Your values
IPspace name	Yes	<ul style="list-style-type: none"> • The IPspace to which the subnet will be assigned. • The IPspace must exist.
Subnet name	Yes	<ul style="list-style-type: none"> • The name of the subnet. • The name must be unique in the IPspace.
Broadcast domain name	Yes	<ul style="list-style-type: none"> • The broadcast domain to which the subnet will be assigned. • The broadcast domain must reside in the specified IPspace.
Subnet name and mask	Yes	<ul style="list-style-type: none"> • The subnet and mask in which the IP addresses reside.
Gateway	No	<ul style="list-style-type: none"> • You can specify a default gateway for the subnet. • If you do not assign a gateway when you create the subnet, you can assign one to the subnet at any time.

Information	Required?	Your values
<p>IP address ranges</p> <ul style="list-style-type: none"> You can specify a range of IP addresses or specific IP addresses. <p>For example, you can specify a range such as:</p> <p style="color: red;">192.168.1.1- 192.168.1.100, 192.168.1.112, 192.168.1.145</p> <ul style="list-style-type: none"> If you do not specify an IP address range, the entire range of IP addresses in the specified subnet are available to assign to LIFs. 	No	
<p>Force update of LIF associations</p> <ul style="list-style-type: none"> Specifies whether to force the update of existing LIF associations. By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided. Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed. 	No	

SVM configuration

You use SVMs to serve data to clients and hosts.

The values you record are for creating a default data SVM. If you are creating a MetroCluster source SVM, see the [Fabric-attached MetroCluster Installation and Configuration Guide](#) or the [Stretch MetroCluster Installation and Configuration Guide](#).

Information	Required?	Your values
SVM name <ul style="list-style-type: none"> The name of the SVM. You should use a fully qualified domain name (FQDN) to ensure unique SVM names across cluster leagues. 	Yes	
Root volume name <ul style="list-style-type: none"> The name of the SVM root volume. 	Yes	
Aggregate name <ul style="list-style-type: none"> The name of the aggregate that holds the SVM root volume. This aggregate must exist. 	Yes	
Security style <ul style="list-style-type: none"> The security style for the SVM root volume. Possible values are ntfs, unix, and mixed. 	Yes	
IPspace name <ul style="list-style-type: none"> The IPspace to which the SVM is assigned. This IPspace must exist. 	No	
SVM language setting <ul style="list-style-type: none"> The default language to use for the SVM and its volumes. If you do not specify a default language, the default SVM language is set to C.UTF-8. The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM. <p>You can modify The language after the SVM is created.</p>	No	

LIF configuration

An SVM serves data to clients and hosts through one or more network logical interfaces (LIFs).

Information	Required?	Your values
SVM name	Yes <ul style="list-style-type: none">• The name of the SVM for the LIF.	
LIF name	Yes <ul style="list-style-type: none">• The name of the LIF.• You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports.• To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes. Important: If you are configuring a SMB server to host Hyper-V or SQL Server over SMB for nondisruptive operation solutions, the SVM must have at least one data LIF on every node in the cluster.	
LIF role	Yes Deprecated from ONTAP 9.6 <ul style="list-style-type: none">• The role of the LIF.• Data LIFs are assigned the data role.	data
Service policy Service policy for the LIF. The service policy defines which network services can use the LIF. Built-in services and service policies are available for managing data and management traffic on both data and system SVMs.	Yes Starting from ONTAP 9.6	

Information	Required?	Your values
<p>Allowed protocols</p> <ul style="list-style-type: none"> The protocols that can use the LIF. By default, CIFS, NFS, and FlexCache are allowed. <p>The FlexCache protocol enables a volume to be used as an origin volume for a FlexCache volume on a system running Data ONTAP operating in 7-Mode.</p> <p> The protocols that use the LIF cannot be modified after the LIF is created. You should specify all protocols when you configure the LIF.</p>	No	
<p>Home node</p> <ul style="list-style-type: none"> The node to which the LIF returns when the LIF is reverted to its home port. You should record a home node for each data LIF. 	Yes	
<p>Home port or broadcast domain</p> <ul style="list-style-type: none"> The port to which the logical interface returns when the LIF is reverted to its home port. You should record a home port for each data LIF. 	Yes	

Information	Required?	Your values
Subnet name <ul style="list-style-type: none"> • The subnet to assign to the SVM. • All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet. 	Yes (if using a subnet)	

DNS configuration

You must configure DNS on the SVM before creating an NFS or SMB server.

Information	Required?	Your values
SVM name <ul style="list-style-type: none"> • The name of the SVM on which you want to create an NFS or SMB server. 	Yes	
DNS domain name <ul style="list-style-type: none"> • A list of domain names to append to a host name when performing host- to-IP name resolution. • List the local domain first, followed by the domain names for which DNS queries are most often made. 	Yes	

Information	Required?	Your values
<p>IP addresses of the DNS servers</p> <p>* List of IP addresses for the DNS servers that will provide name resolution for the NFS or SMB server.</p> <p>* The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the SMB server will join.</p> <p>The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. SMB server creation fails if ONTAP cannot obtain the service location records through local DNS queries.</p> <p>The simplest way to ensure that ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers.</p> <p>You can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers.</p> <p>* For information about the Active Directory-integrated SRV records, see the topic How DNS Support for Active Directory Works on Microsoft TechNet.</p>	Yes	

Dynamic DNS configuration

Before you can use dynamic DNS to automatically add DNS entries to your Active Directory- integrated DNS servers, you must configure dynamic DNS (DDNS) on the SVM.

DNS records are created for every data LIF on the SVM. By creating multiple data LIFS on the SVM, you can load-balance client connections to the assigned data IP addresses. DNS load balances connections that are made using the host name to the assigned IP addresses in a round- robin fashion.

Information	Required?	Your values
SVM name	Yes	
<ul style="list-style-type: none"> The SVM on which you want to create an NFS or SMB server. 		
Whether to use DDNS	Yes	
<ul style="list-style-type: none"> Specifies whether to use DDNS. The DNS servers configured on the SVM must support DDNS. By default, DDNS is disabled. 		
Whether to use secure DDNS	No	
<ul style="list-style-type: none"> Secure DDNS is supported only with Active Directory-integrated DNS. If your Active Directory-integrated DNS allows only secure DDNS updates, the value for this parameter must be true. By default, secure DDNS is disabled. Secure DDNS can be enabled only after a SMB server or an Active Directory account has been created for the SVM. 		
FQDN of the DNS domain	No	
<ul style="list-style-type: none"> The FQDN of the DNS domain. You must use the same domain name configured for DNS name services on the SVM. 		

Create IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Before you begin

You must be a cluster administrator to perform this task.

Step

Create an IPspace.

```
network ipspace create -ipspace ipspace1
```

```
network ipspace show
```

IPspace	Vserver List	Broadcast Domains
Cluster	Cluster	Cluster
Default	Cluster1	Default
ipspace1	ipspace1	-

The IPspace is created, along with the system SVM for the IPspace. The system SVM carries management traffic.

Determining which ports can be used for a broadcast domain

Before you can configure a broadcast domain to add to the new IPspace, you must determine what ports are available for the broadcast domain.



This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- Ports can be physical ports, VLANs, or interface groups (ifgroups).
- The ports that you want to add to the new broadcast domain cannot be assigned to an existing broadcast domain.
- If the ports that you want to add to the broadcast domain are already in another broadcast domain (for example, the Default broadcast domain in the Default IPspace), you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.
- Ports that have LIFs assigned to them cannot be removed from a broadcast domain.
- Because the cluster management and node management LIFs are assigned to the Default broadcast domain in the Default IPspace, the ports assigned to these LIFs cannot be removed from the Default broadcast domain.

Steps

1. Determine the current port assignments.

```
network port show
```

Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper
<hr/>						
node1	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
node2	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

In this example, the output from the command provides the following information:

- Ports **e0c**, **e0d**, **e0e**, **e0f**, and **e0g** on each node are assigned to the Default broadcast domain.
- These ports are potentially available to use in the broadcast domain of the IPspace that you want to create.

2. Determine which ports in the Default broadcast domain are assigned to LIF interfaces, and therefore cannot be moved to a new broadcast domain.

network interface show

Vserver	Logical Interface	Status	Network Admin/Oper Address/Mask	Current Node	Current Port	Is Home
<hr/>						
Cluster	node1_clus1	up/up	10.0.2.40/24	node1	e0a	true
	node1_clus2	up/up	10.0.2.41/24	node1	e0b	true
	node2_clus1	up/up	10.0.2.42/24	node2	e0a	true
	node2_clus2	up/up	10.0.2.43/24	node2	e0b	true
<hr/>						
cluster1	cluster_mgmt	up/up	10.0.1.41/24	node1	e0c	true
	node1_mgmt	up/up	10.0.1.42/24	node1	e0c	true
	node2_mgmt	up/up	10.0.1.43/24	node2	e0c	true

In the following example, the output from the command provides the following information:

- The node ports are assigned to port `e0c` on each node and the cluster administrative LIF's home node is on `e0c` on `node1`.
- Ports `e0d`, `e0e`, `e0f`, and `e0g` on each node are not hosting LIFs and can be removed from the Default broadcast domain and then added to a new broadcast domain for the new IPspace.

Remove ports from a broadcast domain

If the ports that you want to add to the new broadcast domain are already in another broadcast domain, you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.



This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Remove ports from the broadcast domain specifying the following:
 - IPspace, `Default` in the following sample.
 - Broadcast domain, `Default` in the following sample.
 - Ports, using the node and port syntax, `node1:e0d, node1:e0e, node2:e0d, node2:e0e` in the following sample.

```
network port broadcast-domain remove-ports -ipspace Default
-broadcast-domain Default -ports
node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

2. Verify that the ports were removed from the broadcast domain:

```
network port show
```

Create a broadcast domain

You must create a broadcast domain for a custom IPspace. The SVMs created in the IPspace use the ports in the broadcast domain.



This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

Before you begin

You must be a cluster administrator to perform this task.

About this task

The port to which a LIF fails over must be a member of the failover group for the LIF. When you create a broadcast domain, ONTAP automatically creates a failover group with the same name. The failover group contains all the ports assigned to the broadcast domain.

Steps

1. Create a broadcast domain.

```
network port broadcast-domain create -ipspace ipspace1 -broadcast-domain  
-ipspace1 -mtu 1500 -ports node1:e0d,node1:e0e,node2:e0d,node2:e0e
```

2. Verify that the broadcast domain configuration is correct.

- a. Verify the broadcast domain is correct:

```
network port broadcast-domain show
```

- b. Verify the network port is correct:

```
network port show
```

- c. Verify the failover group names and failover targets are correct:

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

Create a subnet

After you create the broadcast domain, you can create a subnet to allocate specific blocks of IPv4 or IPv6 addresses to be used later when you create LIFs for the SVM.

This enables you to create LIFs more easily by specifying a subnet name instead of having to specify IP address and network mask values for each LIF.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Create a subnet.

```
network subnet create -broadcast-domain ipspace1 -ipspace ipspace1  
-subnet-name ipspace1 -subnet 10.0.0.0/24 -gateway 10.0.0.1 -ip-ranges  
"10.0.0.128-10.0.0.130,10.0.0.132"
```

The subnet name can be either a subnet IP value such as `192.0.2.0/24` or a string such as `ipspace1` like the one used in this example.

2. Verify that the subnet configuration is correct.

The output from this example shows information about the subnet named `ipspace1` in the `ipspace1` IPspace. The subnet belongs to the broadcast domain name `ipspace1`. You can assign the IP addresses in this subnet to data LIFs for SVMs created in the `ipspace1` IPspace.

```
network subnet show -ipspace ipspace1
```

Create SVMs

You must create an SVM to serve data to clients.

Before you begin

- You must be a cluster administrator to perform this task.
- You must know which security style the SVM root volume will have.

If you plan to implement a Hyper-V or SQL Server over SMB solution on this SVM, you should use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style data volumes.

Steps

1. Determine which aggregates are candidates for containing the SVM root volume.

```
storage aggregate show -has-mroot false
```

You must choose an aggregate that has at least 1 GB of free space to contain the root volume. If you intend to configure NAS auditing on the SVM, you must have a minimum of 3 GB of extra free space on the root aggregate, with the extra space being used to create the auditing staging volume when auditing is enabled.



If NAS auditing is already enabled on an existing SVM, the aggregate's staging volume is created immediately after aggregate creation is successfully completed.

2. Record the name of the aggregate on which you want to create the SVM root volume.
3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:

```
vserver create -language ?
```

4. If you plan on specifying a Snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the Snapshot policy you want to use:

```
volume snapshot policy show -vserver <vserver_name>
```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume quota policy show -vserver <vserver_name>
```

6. Create an SVM:

```
vserver create -vserver <vserver_name> -aggregate <aggregate_name> -rootvolume <root_volume_name> -rootvolume-security-style {unix|ntfs|mixed} [-ipspace <IPspace_name>] [-language <language>] [-snapshot-policy <snapshot_policy_name>] [-quota-policy <quota_policy_name>] [-comment <comment>]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root -rootvolume-security-style ntfs -ipspace ipspace1 -language en_US.UTF-8
```

[Job 72] Job succeeded: Vserver creation completed

7. Verify that the SVM configuration is correct.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In this example, the command creates the SVM named "vs1" in IPspace "ipspace1". The root volume is named "vs1_root" and is created on aggr3 with NTFS security style.

Create LIFs

An SVM serves data to clients through one or more network logical interfaces (LIFs). You must create LIFs on the ports you want to use to access data.

Before you begin

You must be a cluster administrator to perform this task.

About this task

Starting with ONTAP 9.7, ONTAP automatically chooses the home port of a LIF, as long as at least one LIF

already exists in the same subnet in that IPspace. ONTAP chooses a home-port in the same broadcast domain as other LIFs in that subnet. You can still specify a home port, but it is no longer required (unless no LIFs yet exist in that subnet in the specified IPspace).

You should not configure LIFs that carry CIFS traffic to automatically revert to their home nodes. This recommendation is mandatory if the CIFS server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.

Steps

1. Determine which broadcast domain ports you want to use for the LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

IPspace	Broadcast	Update		
Name	Domain name	MTU	Port List	Status Details
ipspace1	default	1500	node1:e0d node1:e0e node2:e0d node2:e0e	complete complete complete complete

2. Verify that the subnet you want to use for the LIFs contains sufficient unused IP addresses.

```
network subnet show -ipspace ipspace1
```

3. Create one or more LIFs on the ports you want to use to access data.

```
network interface create -vserver vs1 -lif lif1 -home-node node1 -home-port e0d -service-policy default-data-files -subnet-name ipspace1
```

4. Verify that the LIF interface configuration is correct.

```
network interface show -vserver vs1
```

Vserver	Logical Interface	Status	Network Address/Mask	Current Node	Current Port	Is Home
vs1	lif1	up/up	10.0.0.128/24	node1	e0d	true

5. Verify that the failover group configuration is as desired.

```
network interface show -failover -vserver vs1
```

	Logical Vserver	Home interface	Failover Node:Port	Failover Policy	Failover Group
vs1		lif1	node1:e0d	system-defined	ipspace1
					Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e

Get more information

You can get help and find more information through various resources, documentation, and forums.

- [Documentation](#) – Release Notes and Guides for this release and previous releases.
- [NetApp TechCommTV](#) – NetApp videos.
- [NetApp resources](#) – Technical Reports and Knowledgebase Articles.
- [NetApp Community](#) – NetApp product and solutions forums.

ONTAP 9 Networking Reference

This networking reference documentation describes how to configure and manage physical and virtual network ports (VLANs and interface groups), LIFs using IPv4 and IPv6, routing, and host-resolution services in clusters; optimize network traffic by load balancing; and monitor the cluster by using SNMP.

Unless otherwise stated, this content applies to all versions of ONTAP 9.

This content describes basic storage network administration. It shows you how to configure physical and virtual network ports (VLANs and interface groups), how to create LIFs using IPv4 and IPv6, how to manage routing and host-resolution services in clusters, how to use load balancing to optimize network traffic, and how to monitor a cluster using SNMP.

You should use this content under the following circumstances:

- You want to understand the range of ONTAP network management capabilities.
- You want to use the CLI, not ONTAP System Manager.

If you require additional configuration or conceptual information, you should choose among the following documentation:

- Conceptual background for network configuration
 - [ONTAP concepts](#)
- NAS file access
 - [NFS management](#)
 - [SMB/CIFS management](#)
- SAN host provisioning

- SAN administration
- Command reference
 - ONTAP 9 commands
- Technical Reports (TRs), which include additional information about ONTAP technology and interaction with external services
 - NetApp Technical Report 4182: Ethernet Storage Design Considerations and Best Practices for Clustered Data ONTAP Configurations

Upgrade considerations

Network features by release

Analyze the impact of network features available with each ONTAP 9 release.

Available beginning	Feature	Description
ONTAP 9.9.1	Cluster resiliency	<p>The following cluster resiliency and diagnostic improvements improve the customer experience:</p> <ul style="list-style-type: none"> • Port monitoring and avoidance: <ul style="list-style-type: none"> ◦ In two-node switchless cluster configurations, the system avoids ports that experience total packet loss (connectivity loss). Previously this functionality was only available in switched configurations. • Automatic node failover: <ul style="list-style-type: none"> ◦ If a node cannot serve data across its cluster network, that node should not own any disks. Instead its HA partner should take over, if the partner is healthy. • Commands to analyze connectivity issues: <ul style="list-style-type: none"> ◦ Use the following command to display which cluster paths are experiencing packet loss: <code>network interface check cluster-connectivity show</code>

Available beginning	Feature	Description
ONTAP 9.9.1	VIP LIF enhancements	<p>The following fields have been added to extend virtual IP (VIP) border gateway protocol (BGP) functionality:</p> <ul style="list-style-type: none"> • -asn or -peer-asn (4-byte value) The attribute itself is not new, but it now uses a 4-byte integer. • -med • -use-peer-as-next-hop <p>The <code>asn_integer</code> parameter specifies the autonomous system number (ASN) or peer ASN.</p> <ul style="list-style-type: none"> • Starting in ONTAP 9.8, ASN for BGP supports a 2-byte non-negative integer. This is a 16-bit number (0 - 64511 available values). • Starting in ONTAP 9.9.1, ASN for BGP supports a 4-byte non-negative integer (65536 - 4294967295). The default ASN is 65501. ASN 23456 is reserved for ONTAP session establishment with peers that do not announce 4-byte ASN capability. <p>You can make advanced route selections with Multi-Exit Discriminator (MED) support for path prioritization. MED is an optional attribute in the BGP update message that tells routers to select the best route for the traffic. The MED is an unsigned 32-bit integer (0 - 4294967295); lower values are preferred.</p> <p>VIP BGP provides default route automation using BGP peer grouping to simplify configuration. ONTAP has a simple way to learn default routes using the BGP peers as next-hop routers when the BGP peer is on the same subnet. To use the feature, set the <code>-use-peer-as-next-hop</code> attribute to <code>true</code>. By default, this attribute is <code>false</code>.</p> <p>Configure virtual IP (VIP) LIFs</p>

Available beginning	Feature	Description
ONTAP 9.8	Auto port placement	<p>ONTAP can automatically configure broadcast domains, select ports, and help configure network interfaces (LIFs), virtual LANs (VLANs), and link aggregation groups (LAGs) based on reachability and network topology detection.</p> <p>When you first create a cluster, ONTAP automatically discovers the networks connected to ports and configures the needed broadcast domains based on layer 2 reachability. You no longer have to configure broadcast domains manually.</p> <p>A new cluster will continue to be created with two IPspaces:</p> <p>Cluster IPspace: Containing one broadcast domain for the cluster interconnect. You should never touch this configuration.</p> <p>Default IPspace: Containing one or more broadcast domains for the remaining ports. Depending on your network topology, ONTAP configures additional broadcast domains as needed: Default-1, Default-2, and so on. You can rename these broadcast domains if desired, but do not modify which ports are configured in these broadcast domains.</p> <p>When you configure network interfaces, the home port selection is optional. If you do not manually select a home port, ONTAP will attempt to assign an appropriate home port in the same broadcast domain as other network interfaces in the same subnet.</p> <p>When creating a VLAN or adding the first port to a newly created LAG, ONTAP will attempt to automatically assign the VLAN or LAG to the appropriate broadcast domain based on its layer 2 reachability.</p> <p>By automatically configuring broadcast domains and ports, ONTAP helps to ensure that clients maintain access to their data during failover to another port or node in the cluster.</p> <p>Finally, ONTAP sends EMS messages when it detects that the port reachability is incorrect and provides the "network port reachability repair" command to automatically repair common misconfigurations.</p>

Available beginning	Feature	Description
ONTAP 9.8	Internet Protocol security (IPsec) over wire encryption	<p>To ensure data is continuously secure and encrypted, even while in transit, ONTAP uses the IPsec protocol in transport mode. IPsec offers data encryption for all IP traffic including the NFS, iSCSI, and SMB/CIFS protocols. IPsec provides the only encryption in flight option for iSCSI traffic.</p> <p>Once IPsec is configured, network traffic between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.</p> <p>Configure IP security (IPsec) over wire encryption</p>
ONTAP 9.8	Virtual IP (VIP) expansion	<p>New fields have been added to the <code>network bgp peer-group</code> command. This expansion allows you to configure two additional Border Gateway Protocol (BGP) attributes for Virtual IP (VIP).</p> <p>AS path prepend: Other factors being equal, BGP prefers to select the route with shortest AS (autonomous system) Path. You can use the optional AS path prepend attribute to repeat an autonomous system number (ASN), which increases the length of the AS path attribute. The route update with the shortest AS path will be selected by the receiver.</p> <p>BGP community: The BGP community attribute is a 32-bit tag that can be assigned to the route updates. Each route update can have one or more BGP community tags. The neighbors receiving the prefix can examine the community value and take actions like filtering or applying specific routing policies for redistribution.</p>
ONTAP 9.8	Switch CLI simplification	<p>To simplify switch commands, the cluster and storage switch CLIs are consolidated. The consolidated switch CLIs include Ethernet switches, FC switches, and ATTO protocol bridges.</p> <p>Instead of using separate "system cluster-switch" and "system storage-switch" commands, you now use "system switch". For the ATTO protocol bridge, instead of using "storage bridge", use "system bridge".</p> <p>Switch health monitoring has similarly expanded to monitor the storage switches as well as the cluster interconnect switch. You can view health information for the cluster interconnect under "cluster_network" in the "client_device" table. You can view health information for a storage switch under "storage_network" in the "client_device" table.</p>

Available beginning	Feature	Description
ONTAP 9.8	IPv6 variable length	<p>The supported IPv6 variable prefix length range has increased from 64 to 1 through 127 bits. A value of bit 128 remains reserved for virtual IP (VIP).</p> <p>When upgrading, non-VIP LIF lengths other than 64 bits are blocked until the last node is updated.</p> <p>When reverting an upgrade, the revert checks any non-VIP LIFs for any prefix other than 64 bits. If found, the check blocks the revert until you delete or modify the offending LIF. VIP LIFs are not checked.</p>
ONTAP 9.7	Automatic service portmap	<p>The portmap service maps RPC services to the ports on which they listen.</p> <p>The portmap service is always accessible in ONTAP 9.3 and earlier, is configurable in ONTAP 9.4 through ONTAP 9.6, and is managed automatically starting in ONTAP 9.7.</p> <p>In ONTAP 9.3 and earlier: The portmap service (<code>rpcbind</code>) is always accessible on port 111 in network configurations that rely on the built-in ONTAP firewall rather than a third-party firewall.</p> <p>From ONTAP 9.4 through ONTAP 9.6: You can modify firewall policies to control whether the portmap service is accessible on particular LIFs.</p> <p>Starting in ONTAP 9.7: The portmap firewall service is eliminated. Instead, the portmap port is opened automatically for all LIFs that support the NFS service.</p> <p>Portmap service configuration</p>
ONTAP 9.7	Cache search	<p>You can cache NIS <code>netgroup.byhost</code> entries using the <code>vserver services name-service nis-domain netgroup-database</code> commands.</p>
ONTAP 9.6	CUBIC	<p>CUBIC is the default TCP congestion control algorithm for ONTAP hardware. CUBIC replaced the ONTAP 9.5 and earlier default TCP congestion control algorithm, NewReno.</p> <p>CUBIC addresses the problems of long, fat networks (LFNs), including high round trip times (RTTs). CUBIC detects and avoids congestion. CUBIC improves performance for most environments.</p>

Available beginning	Feature	Description
ONTAP 9.6	LIF service policies replace LIF roles	<p>You can assign service policies (instead of LIF roles) to LIFs that determine the kind of traffic that is supported for the LIFs. Service policies define a collection of network services supported by a LIF. ONTAP provides a set of built-in service policies that can be associated with a LIF.</p> <p>ONTAP supports service policies starting with ONTAP 9.5; however, service policies can only be used to configure a limited number of services. Starting with ONTAP 9.6, LIF roles are deprecated and service policies are supported for all types of services.</p> <p>LIFs and service policies</p>
ONTAP 9.5	NTPv3 support	Network Time Protocol (NTP) version 3 includes symmetric authentication using SHA-1 keys, which increases network security.
ONTAP 9.5	SSH login security alerts	When you log in as a Secure Shell (SSH) admin user, you can view information about previous logins, unsuccessful attempts to log in, and changes to your role and privileges since your last successful login.
ONTAP 9.5	LIF service policies	<p>You can create new service policies or use a built-in policy. You can assign a service policy to one or more LIFs; thereby allowing the LIF to carry traffic for a single service or a list of services.</p> <p>LIFs and service policies</p>
ONTAP 9.5	VIP LIFs and BGP support	<p>A VIP data LIF is a LIF that is not part of any subnet and is reachable from all ports that host a border gateway protocol (BGP) LIF in the same IPspace. A VIP data LIF eliminates the dependency of a host on individual network interfaces.</p> <p>Create a virtual IP (VIP) data LIF</p>
ONTAP 9.5	Multipath routing	<p>Multipath routing provides load balancing by utilizing all the available routes to a destination.</p> <p>Enable multipath routing</p>

Available beginning	Feature	Description
ONTAP 9.4	Portmap service	<p>The portmap service maps remote procedure call (RPC) services to the ports on which they listen.</p> <p>The portmap service is always accessible in ONTAP 9.3 and earlier. Starting in ONTAP 9.4, the portmap service is configurable.</p> <p>You can modify firewall policies to control whether the portmap service is accessible on particular LIFs.</p> <p>Portmap service configuration</p>
ONTAP 9.4	SSH MFA for LDAP or NIS	SSH multi-factor authentication (MFA) for LDAP or NIS uses a public key and nsswitch to authenticate remote users.
ONTAP 9.3	SSH MFA	SSH MFA for local administrator accounts use a public key and a password to authenticate local users.
ONTAP 9.3	SAML authentication	You can use Security Assertion Markup Language (SAML) authentication to configure MFA for web services such as Service Processor Infrastructure (spi), ONTAP APIs, and OnCommand System Manager.
ONTAP 9.2	SSH login attempts	You can configure the maximum number of unsuccessful SSH login attempts to protect against brute force attacks.
ONTAP 9.2	Digital security certificates	ONTAP provides enhanced support for digital certificate security with Online Certificate Status Protocol (OCSP) and pre-installed default security certificates.
ONTAP 9.2	Fastpath	<p>As part of a networking stack update for improved performance and resiliency, fast path routing support was removed in ONTAP 9.2 and later releases because it made it difficult to identify problems with improper routing tables. Therefore, it is no longer possible to set the following option in the nodeshell, and existing fast path configurations are disabled when upgrading to ONTAP 9.2 and later:</p> <p><code>ip.fastpath.enable</code></p> <p>Network traffic not sent or sent out of an unexpected interface after upgrade to 9.2 due to elimination of IP Fastpath</p>

Available beginning	Feature	Description
ONTAP 9.1	Security with SNMPv3 traphosts	<p>You can configure SNMPv3 traphosts with the User-based Security Model (USM) security. With this enhancement, SNMPv3 traps can be generated by using a predefined USM user's authentication and privacy credentials.</p> <p>Configure traphosts to receive SNMP notifications</p>
ONTAP 9.0	IPv6	<p>Dynamic DNS (DDNS) name service is available on IPv6 LIFs.</p> <p>Create a LIF</p>
ONTAP 9.0	LIFs per node	<p>The supported number of LIFs per node has increased for some systems. See the Hardware Universe for the number of LIFs supported on each platform for a specified ONTAP release.</p> <p>Create a LIF</p> <p>NetApp hardware universe</p>
ONTAP 9.0	LIF management	<p>ONTAP and System Manager automatically detect and isolate network port failures. LIFs are automatically migrated from degraded ports to healthy ports.</p> <p>Monitor the health of network ports</p>
ONTAP 9.0	LLDP	<p>Link Layer Discovery Protocol (LLDP) provides a vendor-neutral interface for verifying and troubleshooting cabling between an ONTAP system and a switch or router. It is an alternative to Cisco Discovery Protocol (CDP), a proprietary link layer protocol developed by Cisco Systems.</p> <p>Enable or Disable LLDP</p>

Available beginning	Feature	Description
ONTAP 9.0	UC compliance with DSCP marking	<p>Unified Capability (UC) compliance with Differentiated Services Code Point (DSCP) marking.</p> <p>Differentiated Services Code Point (DSCP) marking is a mechanism for classifying and managing network traffic and is a component of Unified Capability (UC) compliance. You can enable DSCP marking on outgoing (egress) IP packet traffic for a given protocol with a default or user-provided DSCP code.</p> <p>If you do not provide a DSCP value when enabling DSCP marking for a given protocol, a default is used:</p> <ul style="list-style-type: none"> 0x0A (10): The default value for data protocols/traffic. 0x30 (48): The default value for control protocols/traffic. <p>DSCP marking for US compliance</p>
ONTAP 9.0	SHA-2 password hash function	<p>To enhance password security, ONTAP 9 supports the SHA-2 password hash function and uses SHA-512 by default for hashing newly created or changed passwords.</p> <p>Existing user accounts with unchanged passwords continue to use the MD5 hash function after the upgrade to ONTAP 9 or later, and users can continue to access their accounts. However, it is strongly recommended that you migrate MD5 accounts to SHA-512 by having users change their passwords.</p>
ONTAP 9.0	FIPS 140-2 support	<p>You can enable the Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces.</p> <p>By default, the FIPS 140-2 only mode is disabled.</p> <p>Configure network security using Federal Information Processing Standards (FIPS)</p>

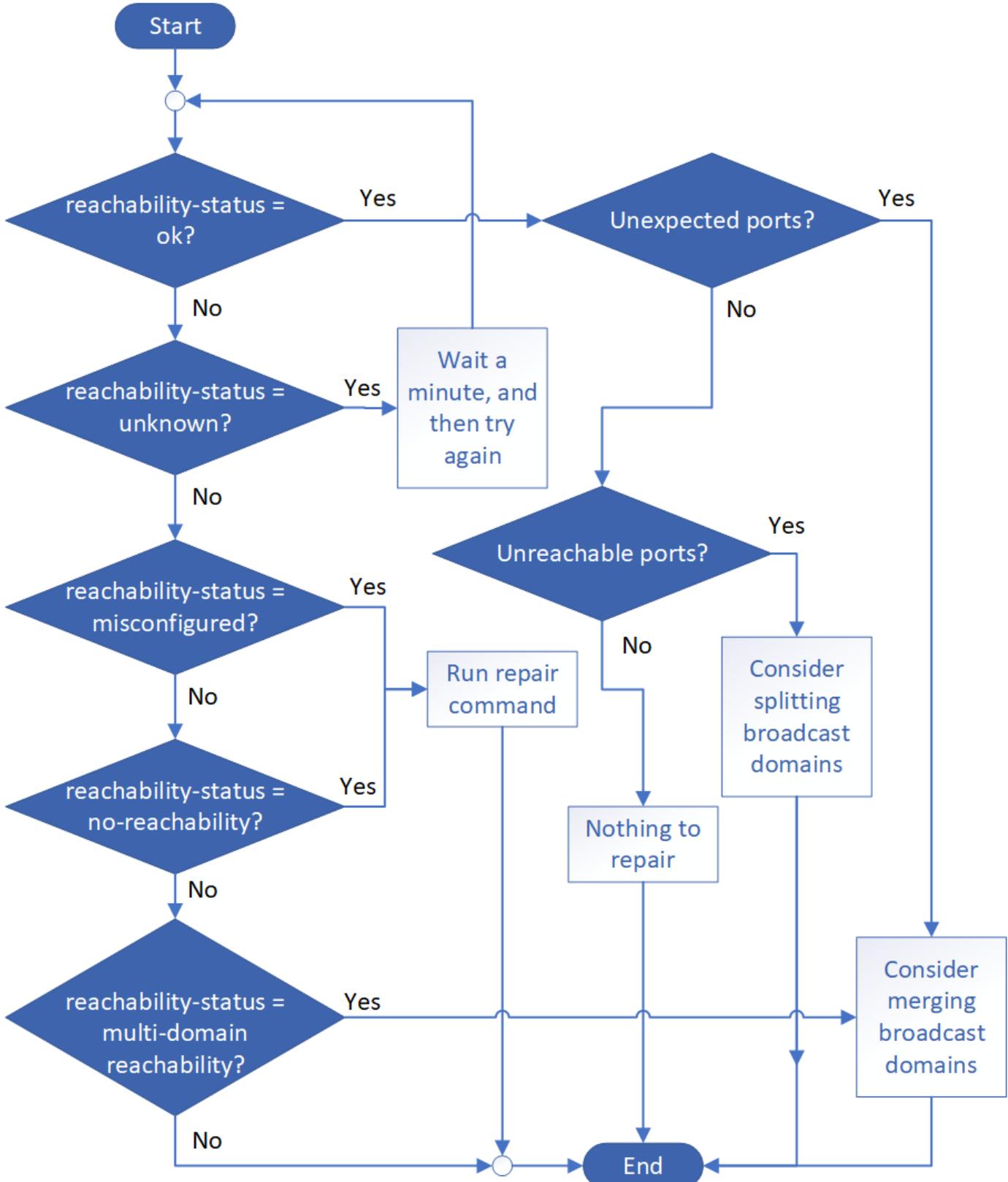
Verify your networking configuration after upgrading to ONTAP 9.8 or later

After an upgrade to ONTAP 9.8, you should verify your network configuration. After the upgrade, ONTAP automatically monitors layer 2 reachability.

Use the following command to verify each port has reachability to its expected broadcast domain:

```
network port reachability show -detail
```

The command output contains reachability results. Use the following decision tree and table to understand the reachability results (reachability-status) and determine what, if anything, to do next.



reachability-status	Description
ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see Merge broadcast domains.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see Split broadcast domains.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see Repair port reachability.</p>
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see Repair port reachability.</p>

reachability-status	Description
multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see Merge broadcast domains or Repair port reachability.</p>
unknown	If the reachability-status is "unknown", then wait a few minutes and try the command again.

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see [Repair port reachability](#).

Networking components of a cluster

Overview

You should familiarize yourself with the networking components of a cluster before setting up the cluster. Configuring the physical networking components of a cluster into logical components provides the flexibility and multi-tenancy functionality in ONTAP.

The various networking components in a cluster are as follows:

- Physical ports

Network interface cards (NICs) and host bus adapters (HBAs) provide physical (Ethernet and Fibre Channel) connections from each node to the physical networks (management and data networks).

For site requirements, switch information, port cabling information, and controller onboard port cabling, see the Hardware Universe at hwu.netapp.com.

- Logical ports

Virtual local area networks (VLANs) and interface groups constitute the logical ports. Interface groups treat several physical ports as a single port, while VLANs subdivide a physical port into multiple separate ports.

- IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

- Broadcast domains

A broadcast domain resides in an IPspace and contains a group of network ports, potentially from many

nodes in the cluster, that belong to the same layer 2 network. The ports in the group are used in an SVM for data traffic.

- Subnets

A subnet is created within a broadcast domain and contains a pool of IP addresses that belong to the same layer 3 subnet. This pool of IP addresses simplifies IP address allocation during LIF creation.

- Logical interfaces

A logical interface (LIF) is an IP address or a worldwide port name (WWPN) that is associated with a port. It is associated with attributes such as failover groups, failover rules, and firewall rules. A LIF communicates over the network through the port (physical or logical) to which it is currently bound.

The different types of LIFs in a cluster are data LIFs, cluster-scoped management LIFs, node-scoped management LIFs, intercluster LIFs, and cluster LIFs. The ownership of the LIFs depends on the SVM where the LIF resides. Data LIFs are owned by data SVMs, node-scoped management LIFs, cluster-scoped management, and intercluster LIFs are owned by the admin SVMs, and cluster LIFs are owned by the cluster SVM.

- DNS zones

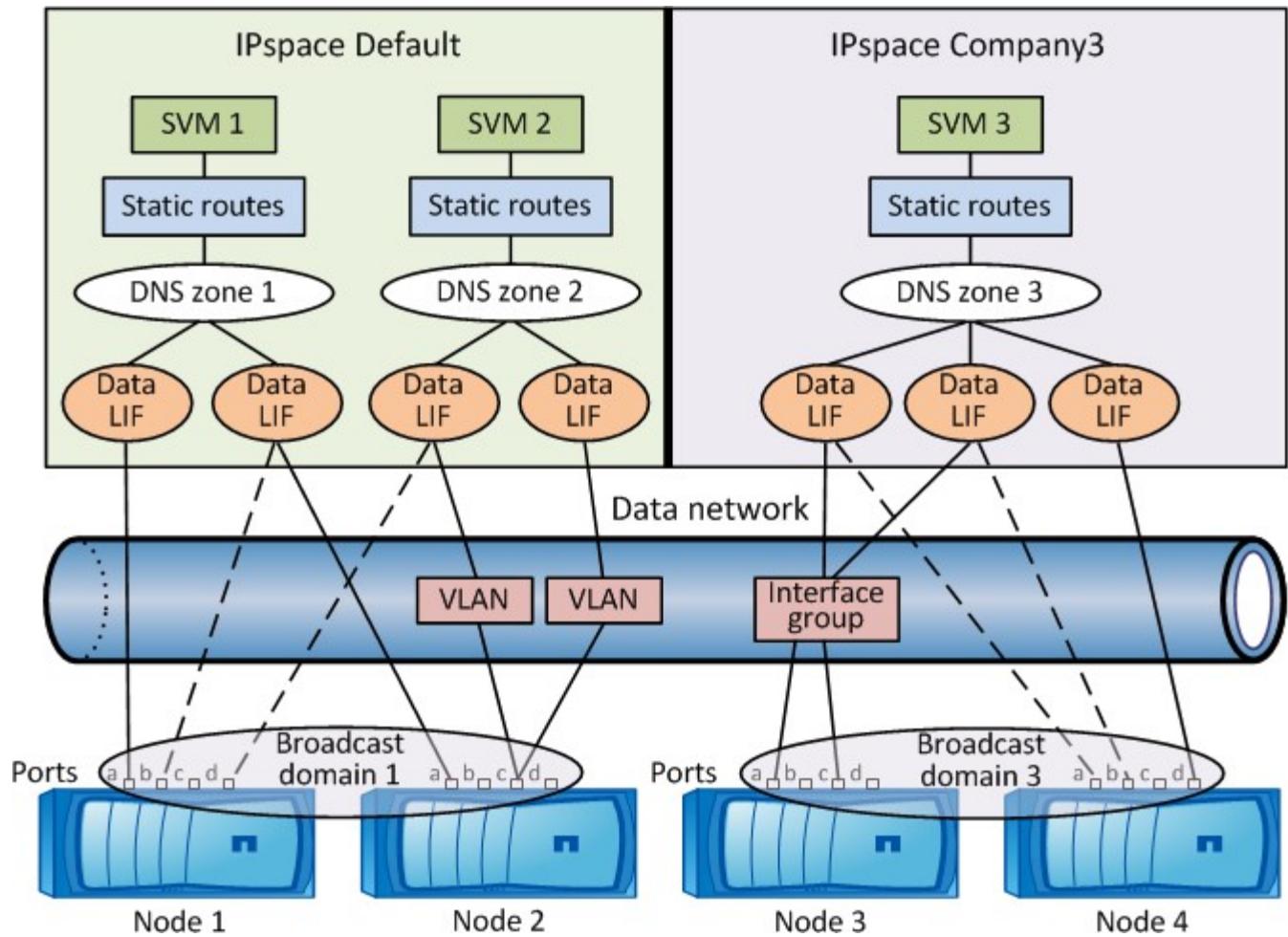
DNS zone can be specified during the LIF creation, providing a name for the LIF to be exported through the cluster's DNS server. Multiple LIFs can share the same name, allowing the DNS load balancing feature to distribute IP addresses for the name according to load.

SVMs can have multiple DNS zones.

- Routing

Each SVM is self-sufficient with respect to networking. An SVM owns LIFs and routes that can reach each of the configured external servers.

The following figure illustrates how the different networking components are associated in a four-node cluster:

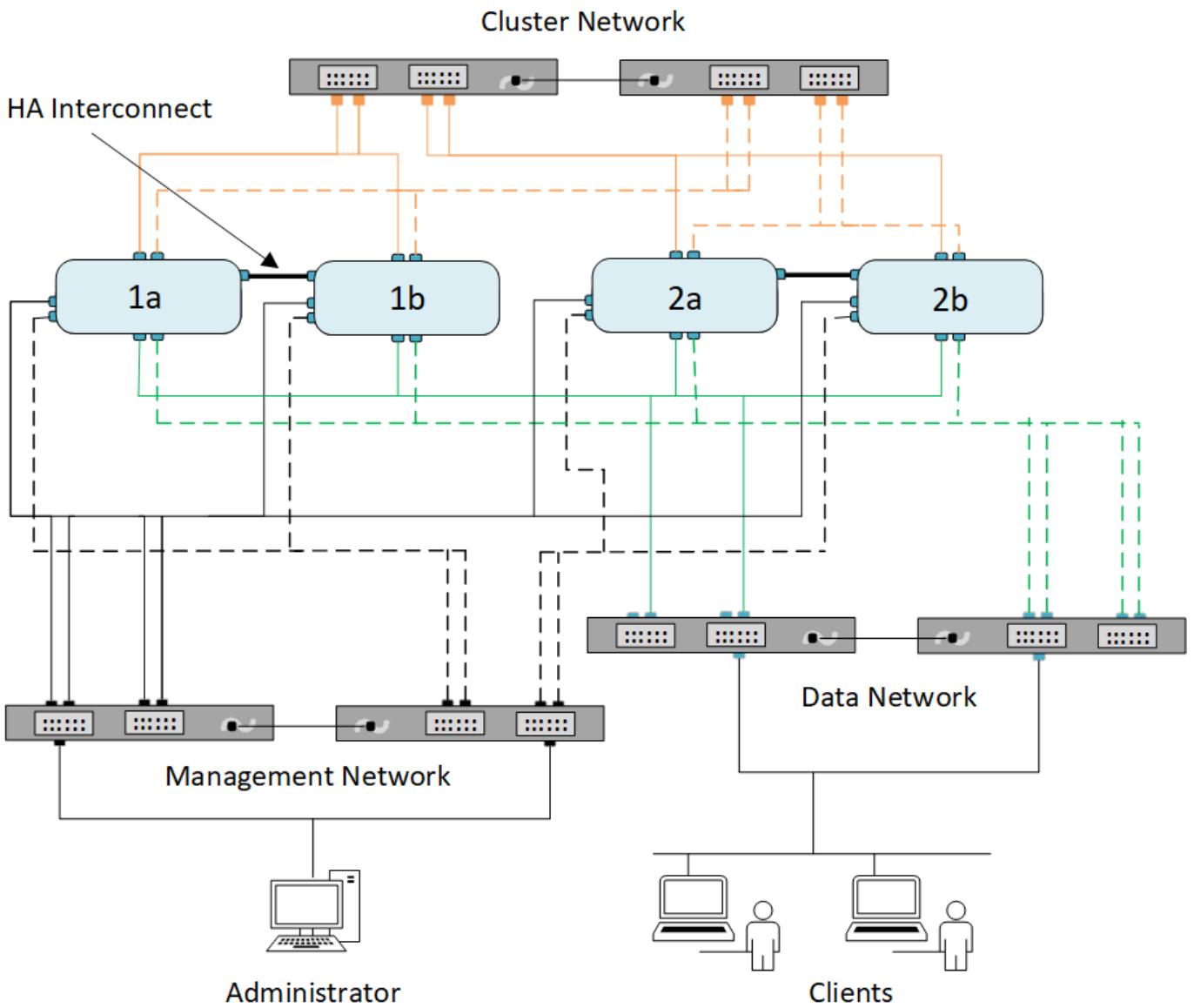


Network cabling guidelines

Network cabling best practices separate traffic into the following networks: cluster, management, and data.

You should cable a cluster so that the cluster traffic is on a separate network from all other traffic. It is an optional, but recommended practice to have network management traffic separated from data and intracluster traffic. By maintaining separate networks, you can achieve better performance, ease of administration, and improved security and management access to the nodes.

The following diagram illustrates the network cabling of a four-node HA cluster that includes three separate networks:



You should follow certain guidelines when cabling network connections:

- Each node should be connected to three distinct networks.

One network is for management, one is for data access, and one is for intracluster communication. The management and data networks can be logically separated.

- You can have more than one data network connection to each node for improving the client (data) traffic flow.
- A cluster can be created without data network connections, but it must include a cluster interconnect connection.
- There should always be two cluster connections to each node, but nodes on FAS22xx systems can be configured with a single 10-GbE cluster port.

For more information on network cabling, see the [AFF and FAS System Documentation Center](#) and the [Hardware Universe](#).

Relationship between broadcast domains, failover groups, and failover policies

Broadcast domains, failover groups, and failover policies work together to determine which port will take over when the node or port on which a LIF is configured fails.

A broadcast domain lists all the ports reachable in the same layer 2 Ethernet network. An Ethernet broadcast packet sent from one of the ports is seen by all other ports in the broadcast domain. This common-reachability characteristic of a broadcast domain is important to LIFs because if a LIF were to fail over to any other port in the broadcast domain, it could still reach every local and remote host that was reachable from the original port.

Failover groups define the ports within a broadcast domain that provide LIF failover coverage for each other. Each broadcast domain has one failover group that includes all its ports. This failover group containing all ports in the broadcast domain is the default and recommended failover group for the LIF. You can create failover groups with smaller subsets that you define, such as a failover group of ports that have the same link speed within a broadcast domain.

A failover policy dictates how a LIF uses the ports of a failover group when a node or port goes down. Consider the failover policy as a type of filter that is applied to a failover group. The failover targets for a LIF (the set of ports to which a LIF can failover) is determined by applying the LIF's failover policy to the LIF's failover group in the broadcast domain.

You can view the failover targets for a LIF using the following CLI command:

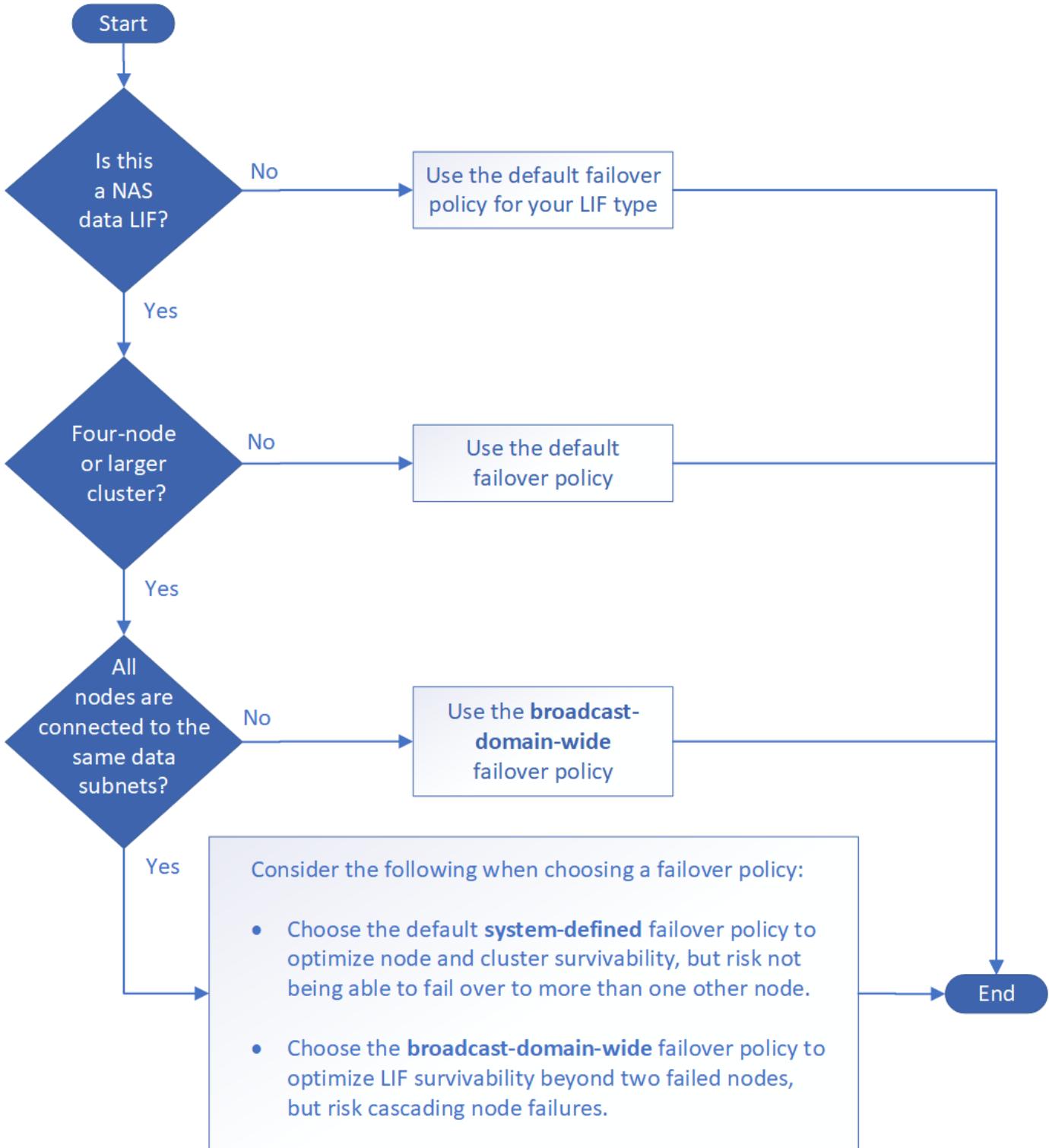
```
network interface show -failover
```

NetApp strongly recommends using the default failover policy for your LIF type.

Decide which LIF failover policy to use

Decide whether to use the recommended, default failover policy or whether to change it based on your LIF type and environment.

Failover policy decision tree



Default failover policies by LIF type

LIF type	Default failover policy	Description
BGP LIFs	disabled	LIF does not fail over to another port.
Cluster LIFs	local-only	LIF fails over to ports on the same node only.

LIF type	Default failover policy	Description
Cluster-mgmt LIF	broadcast-domain-wide	LIF fails over to ports in the same broadcast domain, on any and every node in the cluster.
Intercluster LIFs	local-only	LIF fails over to ports on the same node only.
NAS data LIFs	system-defined	LIF fails over to one other node that is not the HA partner.
Node management LIFs	local-only	LIF fails over to ports on the same node only.
SAN data LIFs	disabled	LIF does not fail over to another port.



The `sfo-partner-only` failover policy is deprecated. Do not use the `sfo-partner-only` failover policy.

Configure network ports (cluster administrators only)

Overview

Ports are either physical ports (NICs) or virtualized ports, such as interface groups or VLANs.

Types of network ports

The network ports are either physical ports or virtualized ports.

Virtual local area networks (VLANs) and interface groups constitute the virtual ports. Interface groups treat several physical ports as a single port, while VLANs subdivide a physical port into multiple separate logical ports.

- Physical ports: LIFs can be configured directly on physical ports.
- Interface group: A port aggregate containing two or more physical ports that act as a single trunk port. An interface group can be single-mode, multimode, or dynamic multimode.
- VLAN: A logical port that receives and sends VLAN-tagged (IEEE 802.1Q standard) traffic. VLAN port characteristics include the VLAN ID for the port. The underlying physical port or interface group ports are considered VLAN trunk ports, and the connected switch ports must be configured to trunk the VLAN IDs.

The underlying physical port or interface group ports for a VLAN port can continue to host LIFs, which transmit and receive untagged traffic.

- Virtual IP (VIP) port: A logical port that is used as the home port for a VIP LIF. VIP ports are created automatically by the system and support only a limited number of operations. VIP ports are supported starting with ONTAP 9.5.

The port naming convention is `enumerletter`:

- The first character describes the port type.

"e" represents Ethernet.

- The second character indicates the numbered slot in which the port adapter is located.
- The third character indicates the port's position on a multiport adapter.
"a" indicates the first port, "b" indicates the second port, and so on.

For example, `e0b` indicates that an Ethernet port is the second port on the node's motherboard.

VLANs must be named by using the syntax `port_name-vlan-id`.

`port_name` specifies the physical port or interface group.

`vlan-id` specifies the VLAN identification on the network. For example, `e1c-80` is a valid VLAN name.

Combine physical ports to create interface groups

An interface group is created by combining two or more physical ports into a single logical port. The logical port provides increased resiliency, increased availability, and load sharing.

Interface group types

Three types of interface groups are supported on the storage system: single-mode, static multimode, and dynamic multimode. Each interface group provides different levels of fault tolerance. Multimode interface groups provide methods for load balancing network traffic.

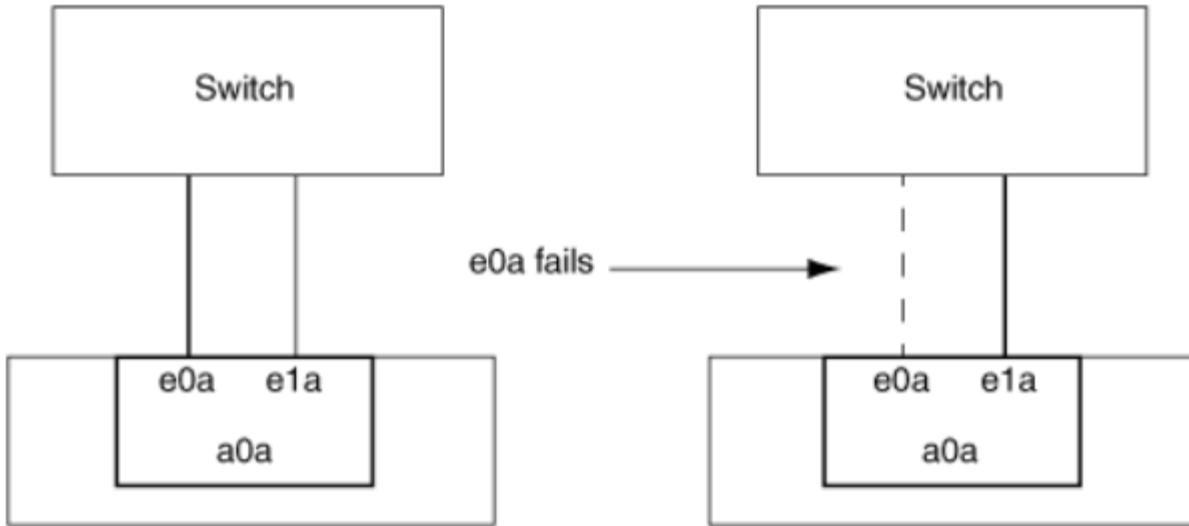
Characteristics of single-mode interface groups

In a single-mode interface group, only one of the interfaces in the interface group is active. The other interfaces are on standby, ready to take over if the active interface fails.

Characteristics of a single-mode interface groups:

- For failover, the cluster monitors the active link and controls failover.
Because the cluster monitors the active link, there is no switch configuration required.
- There can be more than one interface on standby in a single-mode interface group.
- If a single-mode interface group spans multiple switches, you must connect the switches with an Inter-Switch link (ISL).
- For a single-mode interface group, the switch ports must be in the same broadcast domain.
- Link-monitoring ARP packets, which have a source address of 0.0.0.0, are sent over the ports to verify that the ports are in the same broadcast domain.

The following figure is an example of a single-mode interface group. In the figure, e0a and e1a are part of the a0a single-mode interface group. If the active interface, e0a, fails, the standby e1a interface takes over and maintains the connection to the switch.



To accomplish single-mode functionality, the recommended approach is to instead use failover groups. By using a failover group, the second port can still be used for other LIFs and need not remain unused. Additionally, failover groups can span more than two ports and can span ports on multiple nodes.

Characteristics of static multimode interface groups

The static multimode interface group implementation in ONTAP complies with IEEE 802.3ad (static). Any switch that supports aggregates, but does not have control packet exchange for configuring an aggregate, can be used with static multimode interface groups.

Static multimode interface groups do not comply with IEEE 802.3ad (dynamic), also known as Link Aggregation Control Protocol (LACP). LACP is equivalent to Port Aggregation Protocol (PAgP), the proprietary link aggregation protocol from Cisco.

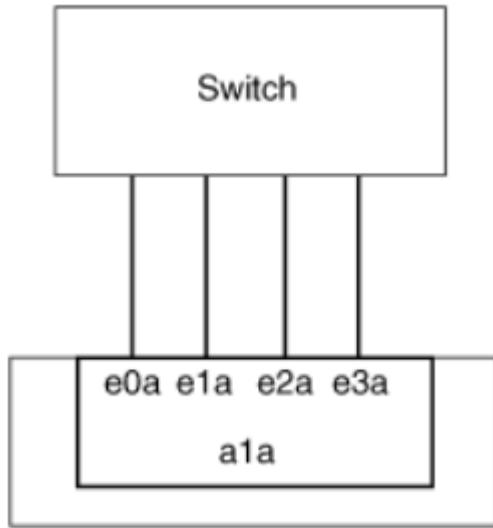
The following are characteristics of a static multimode interface group:

- All interfaces in the interface group are active and share a single MAC address.
 - Multiple individual connections are distributed among the interfaces in the interface group.
 - Each connection or session uses one interface within the interface group.

When you use the sequential load balancing scheme, all sessions are distributed across available links on a packet-by-packet basis, and are not bound to a particular interface from the interface group.
- Static multimode interface groups can recover from a failure of up to "n-1" interfaces, where n is the total number of interfaces that form the interface group.
- If a port fails or is unplugged, the traffic that was traversing the failed link is automatically redistributed to one of the remaining interfaces.
- Static multimode interface groups can detect a loss of link, but they cannot detect a loss of connectivity to the client or switch misconfigurations that might impact connectivity and performance.
- A static multimode interface group requires a switch that supports link aggregation over multiple switch ports.
The switch is configured so that all ports to which links of an interface group are connected are part of a single logical port. Some switches might not support link aggregation of ports configured for jumbo frames. For more information, see your switch vendor's documentation.
- Several load balancing options are available to distribute traffic among the interfaces of a static multimode

interface group.

The following figure is an example of a static multimode interface group. Interfaces e0a, e1a, e2a, and e3a are part of the a1a multimode interface group. All four interfaces in the a1a multimode interface group are active.



Several technologies exist that enable traffic in a single aggregated link to be distributed across multiple physical switches. The technologies used to enable this capability vary among networking products. Static multimode interface groups in ONTAP conform to the IEEE 802.3 standards. If a particular multiple switch link aggregation technology is said to interoperate with or conform to the IEEE 802.3 standards, it should operate with ONTAP.

The IEEE 802.3 standard states that the transmitting device in an aggregated link determines the physical interface for transmission. Therefore, ONTAP is only responsible for distributing outbound traffic, and cannot control how inbound frames arrive. If you want to manage or control the transmission of inbound traffic on an aggregated link, that transmission must be modified on the directly connected network device.

Dynamic multimode interface group

Dynamic multimode interface groups implement Link Aggregation Control Protocol (LACP) to communicate group membership to the directly attached switch. LACP enables you to detect the loss of link status and the inability of the node to communicate with the direct-attached switch port.

Dynamic multimode interface group implementation in ONTAP complies with IEEE 802.3 AD (802.1 AX). ONTAP does not support Port Aggregation Protocol (PAgP), which is a proprietary link aggregation protocol from Cisco.

A dynamic multimode interface group requires a switch that supports LACP.

ONTAP implements LACP in nonconfigurable active mode that works well with switches that are configured in either active or passive mode. ONTAP implements the long and short LACP timers (for use with nonconfigurable values 3 seconds and 90 seconds), as specified in IEEE 802.3 AD (802.1AX).

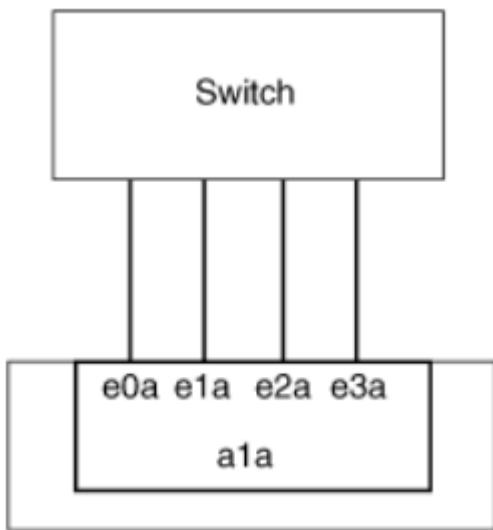
The ONTAP load balancing algorithm determines the member port to be used to transmit outbound traffic, and does not control how inbound frames are received. The switch determines the member (individual physical port) of its port channel group to be used for transmission, based on the load balancing algorithm configured in the switch's port channel group. Therefore, the switch configuration determines the member port (individual physical port) of the storage system to receive traffic. For more information about configuring the switch, see the documentation from your switch vendor.

If an individual interface fails to receive successive LACP protocol packets, then that individual interface is marked as "lag_inactive" in the output of "ifgrp status" command. Existing traffic is automatically rerouted to any remaining active interfaces.

The following rules apply when using dynamic multimode interface groups:

- Dynamic multimode interface groups should be configured to use the port-based, IP-based, MAC-based, or round robin load balancing methods.
- In a dynamic multimode interface group, all interfaces must be active and share a single MAC address.

The following figure is an example of a dynamic multimode interface group. Interfaces e0a, e1a, e2a, and e3a are part of the a1a multimode interface group. All four interfaces in the a1a dynamic multimode interface group are active.



Load balancing in multimode interface groups

You can ensure that all interfaces of a multimode interface group are equally utilized for outgoing traffic by using the IP address, MAC address, sequential, or port-based load balancing methods to distribute network traffic equally over the network ports of a multimode interface group.

The load balancing method for a multimode interface group can be specified only when the interface group is created.

Best Practice: Port-based load balancing is recommended whenever possible. Use port-based load balancing unless there is a specific reason or limitation in the network that prevents it.

Port-based load balancing

Port-based load balancing is the recommended method.

You can equalize traffic on a multimode interface group based on the transport layer (TCP/UDP) ports by using the port-based load balancing method.

The port-based load balancing method uses a fast hashing algorithm on the source and destination IP addresses along with the transport layer port number.

IP address and MAC address load balancing

IP address and MAC address load balancing are the methods for equalizing traffic on multimode interface groups.

These load balancing methods use a fast hashing algorithm on the source and destination addresses (IP address and MAC address). If the result of the hashing algorithm maps to an interface that is not in the UP link-state, the next active interface is used.



Do not select the MAC address load balancing method when creating interface groups on a system that connects directly to a router. In such a setup, for every outgoing IP frame, the destination MAC address is the MAC address of the router. As a result, only one interface of the interface group is used.

IP address load balancing works in the same way for both IPv4 and IPv6 addresses.

Sequential load balancing

You can use sequential load balancing to equally distribute packets among multiple links using a round robin algorithm. You can use the sequential option for load balancing a single connection's traffic across multiple links to increase single connection throughput.

However, because sequential load balancing may cause out-of-order packet delivery, extremely poor performance can result. Therefore, sequential load balancing is generally not recommended.

Create an interface group

You can create an interface group—single-mode, static multimode, or dynamic multimode (LACP)—to present a single interface to clients by combining the capabilities of the aggregated network ports.

About this task

- For a complete list of configuration restrictions that apply to port interface groups, see the [network port ifgrp add-port](#) man page.
- When creating a multimode interface group, you can specify any of the following load-balancing methods:
 - port: Network traffic is distributed on the basis of the transport layer (TCP/UDP) ports. This is the recommended load-balancing method.
 - mac: Network traffic is distributed on the basis of MAC addresses.
 - ip: Network traffic is distributed on the basis of IP addresses.
 - sequential: Network traffic is distributed as it is received.



The MAC address of an interface group is determined by the order of the underlying ports and how these ports initialize during bootup. You should therefore not assume that the ifgrp MAC address is persistent across reboots or ONTAP upgrades.

Step

Use the [network port ifgrp create](#) command to create an interface group.

Interface groups must be named using the syntax `a<number><letter>`. For example, a0a, a0b, a1c, and a2a are valid interface group names.

For more information about this command, see [ONTAP 9 commands](#).

The following example shows how to create an interface group named a0a with a distribution function of port and a mode of multimode:

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

Add a port to an interface group

You can add up to 16 physical ports to an interface group for all port speeds.

Step

Add network ports to the interface group:

```
network port ifgrp add-port
```

For more information about this command, see [ONTAP 9 commands](#).

The following example shows how to add port e0c to an interface group named a0a:

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Starting in ONTAP 9.8, interface groups are automatically placed into an appropriate broadcast domain about one minute after the first physical port is added to the interface group. If you do not want ONTAP to do this, and prefer to manually place the ifgrp into a broadcast domain, then specify the `-skip-broadcast-domain-placement` parameter as part of the `ifgrp add-port` command.

Remove a port from an interface group

You can remove a port from an interface group that hosts LIFs, as long as it is not the last port in the interface group. There is no requirement that the interface group must not host LIFs or that the interface group must not be the home port of a LIF considering that you are not removing the last port from the interface group. However, if you are removing the last port, then you must migrate or move the LIFs from the interface group first.

About this task

You can remove up to 16 ports (physical interfaces) from an interface group.

Step

Remove network ports from an interface group:

```
network port ifgrp remove-port
```

The following example shows how to remove port e0c from an interface group named a0a:

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Delete an interface group

You can delete interface groups if you want to configure LIFs directly on the underlying physical ports or decide to change the interface group mode or distribution function.

Before you begin

- The interface group must not be hosting a LIF.

- The interface group must be neither the home port nor the failover target of a LIF.

Step

Use the `network port ifgrp delete` command to delete an interface group.

For more information about this command, see [ONTAP 9 commands](#).

The following example shows how to delete an interface group named a0b:

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

Configure VLANs over physical ports

VLANs provide logical segmentation of networks by creating separate broadcast domains that are defined on a switch port basis as opposed to the traditional broadcast domains, defined on physical boundaries.

A VLAN can span multiple physical network segments. The end-stations belonging to a VLAN are related by function or application.

For example, end-stations in a VLAN might be grouped by departments, such as engineering and accounting, or by projects, such as release1 and release2. Because physical proximity of the end-stations is not essential in a VLAN, you can disperse the end-stations geographically and still contain the broadcast domain in a switched network.

You can manage VLANs by creating, deleting, or displaying information about them.



You should not create a VLAN on a network interface with the same identifier as the native VLAN of the switch. For example, if the network interface e0b is on native VLAN 10, you should not create a VLAN e0b-10 on that interface.

Create a VLAN

You can create a VLAN for maintaining separate broadcast domains within the same network domain by using the `network port vlan create` command.

Before you begin

Your network administrator must have confirmed that the following requirements have been met:

- The switches deployed in the network must either comply with IEEE 802.1Q standards or have a vendor-specific implementation of VLANs.
- For supporting multiple VLANs, an end-station must be statically configured to belong to one or more VLANs.
- The VLAN is not attached to a port hosting a cluster LIF.
- The VLAN is not attached to ports assigned to the Cluster IPspace.
- The VLAN is not created on an interface group port that contains no member ports.

About this task

In certain circumstances, if you want to create the VLAN port on a degraded port without correcting the hardware issue or any software misconfiguration, then you can set the `-ignore-health-status` parameter of the `network port modify` command as true.

Creating a VLAN attaches the VLAN to the network port on a specified node in a cluster.

When you configure a VLAN over a port for the first time, the port might go down, resulting in a temporary disconnection of the network. Subsequent VLAN additions to the same port do not affect the port state.



You should not create a VLAN on a network interface with the same identifier as the native VLAN of the switch. For example, if the network interface e0b is on native VLAN 10, you should not create a VLAN e0b-10 on that interface.

Step

1. Use the `network port vlan create` command to create a VLAN.
2. You must specify either the `vlan-name` or the `port` and `vlan-id` options when creating a VLAN. The VLAN name is a combination of the name of the port (or interface group) and the network switch VLAN identifier, with a hyphen in between. For example, `e0c-24` and `e1c-80` are valid VLAN names.

The following example shows how to create a VLAN `e1c-80` attached to network port `e1c` on the node `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

Starting with ONTAP 9.8, VLANs are automatically placed into appropriate broadcast domains about one minute after their creation. If you do not want ONTAP to do this, and prefer to manually place the VLAN into a broadcast domain, then specify the `-skip-broadcast-domain-placement` parameter as part of the `vlan create` command.

For more information about this command, see [ONTAP 9 commands](#).

Delete a VLAN

You might have to delete a VLAN before removing a NIC from its slot. When you delete a VLAN, it is automatically removed from all of the failover rules and groups that use it.

Before you begin

Make sure there are no LIFs associated with the VLAN.

About this task

Deletion of the last VLAN from a port might cause a temporary disconnection of the network from the port.

Step

Use the `network port vlan delete` command to delete a VLAN.

The following example shows how to delete VLAN `e1c-80` from network port `e1c` on the node `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

Modify network port attributes

You can modify the autonegotiation, duplex, flow control, speed, and health settings of a physical network port.

Before you begin

The port that you want to modify must not be hosting any LIFs.

About this task

- You should not modify the administrative settings of the 100 GbE, 40 GbE, 10 GbE or 1 GbE network interfaces.

The values that you can set for duplex mode and port speed are referred to as administrative settings. Depending on network limitations, the administrative settings can differ from the operational settings (that is, the duplex mode and speed that the port actually uses).

- You should not modify the administrative settings of the underlying physical ports in an interface group.

The `-up-admin` parameter (available at the advanced privilege level) modifies the administrative settings of the port.

- The `-up-admin` administrative setting should not be set to false for all ports on a node, or for the port that hosts the last operational cluster LIF on a node.
- You should not modify the MTU size of the management port, `e0M`.
- The MTU size of a port in a broadcast domain cannot be changed from the MTU value that is set for the broadcast domain.
- The MTU size of a VLAN cannot exceed the value of the MTU size of its base port.

Steps

1. Modify the attributes of a network port:

```
network port modify
```

2. You can set the `-ignore-health-status` field to true for specifying that the system can ignore the network port health status of a specified port.

The network port health status is automatically changed from degraded to healthy, and this port can now be used for hosting LIFs. You should set the flow control of cluster ports to `none`. By default, the flow control is set to `full`.

The following command disables the flow control on port `e0b` by setting the flow control to `none`:

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

Modify MTU setting for interface group ports

To modify the MTU setting for interface groups, you must modify the MTU of the broadcast domain.

Steps

1. Modify the broadcast domain settings:

```
broadcast-domain modify -broadcast-domain broadcast_domain_name -mtu  
mtu_setting
```

The following warning message is displayed:

```
Warning: Changing broadcast domain settings will cause a momentary data-  
serving interruption.  
Do you want to continue? {y|n}: y
```

2. Enter y to continue.

3. Verify that the MTU setting were modified correctly:

```
net port show
```

```
net port show  
(network port show)  
Node: vsim-01
```

Port	IPspace	Broadcast Domain	Link	MTU	Speed (Mbps)	Admin/Oper	Health	Status	Ignore	Health	Status
a0a	Default	Default-1	up	1300	auto/1000	healthy	healthy	false			
e0a	Default	Default-1	up	1300	auto/1000	healthy	healthy	false			
e0b	Default	Default	up	1500	auto/1000	healthy	healthy	false			
e0c	Default	Default	up	1500	auto/1000	healthy	healthy	false			
e0d	Default	Default	up	1500	auto/1000	healthy	healthy	false			

5 entries were displayed.

Monitor the health of network ports

ONTAP management of network ports includes automatic health monitoring and a set of health monitors to help you identify network ports that might not be suitable for hosting LIFs.

About this task

If a health monitor determines that a network port is unhealthy, it warns administrators through an EMS message or marks the port as degraded. ONTAP avoids hosting LIFs on degraded network ports if there are healthy alternative failover targets for that LIF. A port can become degraded because of a soft failure event, such as link flapping (links bouncing quickly between up and down) or network partitioning:

- Network ports in the cluster IPspace are marked as degraded when they experience link flapping or loss of layer 2 (L2) reachability to other network ports in the broadcast domain.
- Network ports in non-cluster IPspaces are marked as degraded when they experience link flapping.

You must be aware of the following behaviors of a degraded port:

- A degraded port cannot be included in a VLAN or an interface group.

If a member port of an interface group is marked as degraded, but the interface group is still marked as healthy, LIFs can be hosted on that interface group.

- LIFs are automatically migrated from degraded ports to healthy ports.
- During a failover event, a degraded port is not considered as the failover target. If no healthy ports are available, degraded ports host LIFs according to the normal failover policy.
- You cannot create, migrate, or revert a LIF to a degraded port.

You can modify the `ignore-health-status` setting of the network port to `true`. You can then host a LIF on the healthy ports.

Steps

1. Log in to the advanced privilege mode:

```
set -privilege advanced
```

2. Check which health monitors are enabled for monitoring network port health:

```
network options port-health-monitor show
```

The health status of a port is determined by the value of health monitors.

The following health monitors are available and enabled by default in ONTAP:

- Link-flapping health monitor: Monitors link flapping

If a port has link flapping more than once in five minutes, this port is marked as degraded.

- L2 reachability health monitor: Monitors whether all ports configured in the same broadcast domain have L2 reachability to each other

This health monitor reports L2 reachability issues in all IPspaces; however, it marks only the ports in the cluster IPspace as degraded.

- CRC monitor: Monitors the CRC statistics on the ports

This health monitor does not mark a port as degraded but generates an EMS message when a very high CRC failure rate is observed.

3. Enable or disable any of the health monitors for an IPspace as desired by using the `network options port-health-monitor modify` command.

4. View the detailed health of a port:

```
network port show -health
```

The command output displays the health status of the port, `ignore health status` setting, and list of reasons the port is marked as degraded.

A port health status can be `healthy` or `degraded`.

If the `ignore health status` setting is `true`, it indicates that the port health status has been modified from `degraded` to `healthy` by the administrator.

If the `ignore health status` setting is `false`, the port health status is determined automatically by the system.

Monitor the reachability of network ports in ONTAP 9.8 and later

Reachability monitoring is built into ONTAP 9.8 and later. Use this monitoring to identify when the physical network topology does not match the ONTAP configuration. In some cases, ONTAP can repair port reachability. In other cases, additional steps are required.

About this task

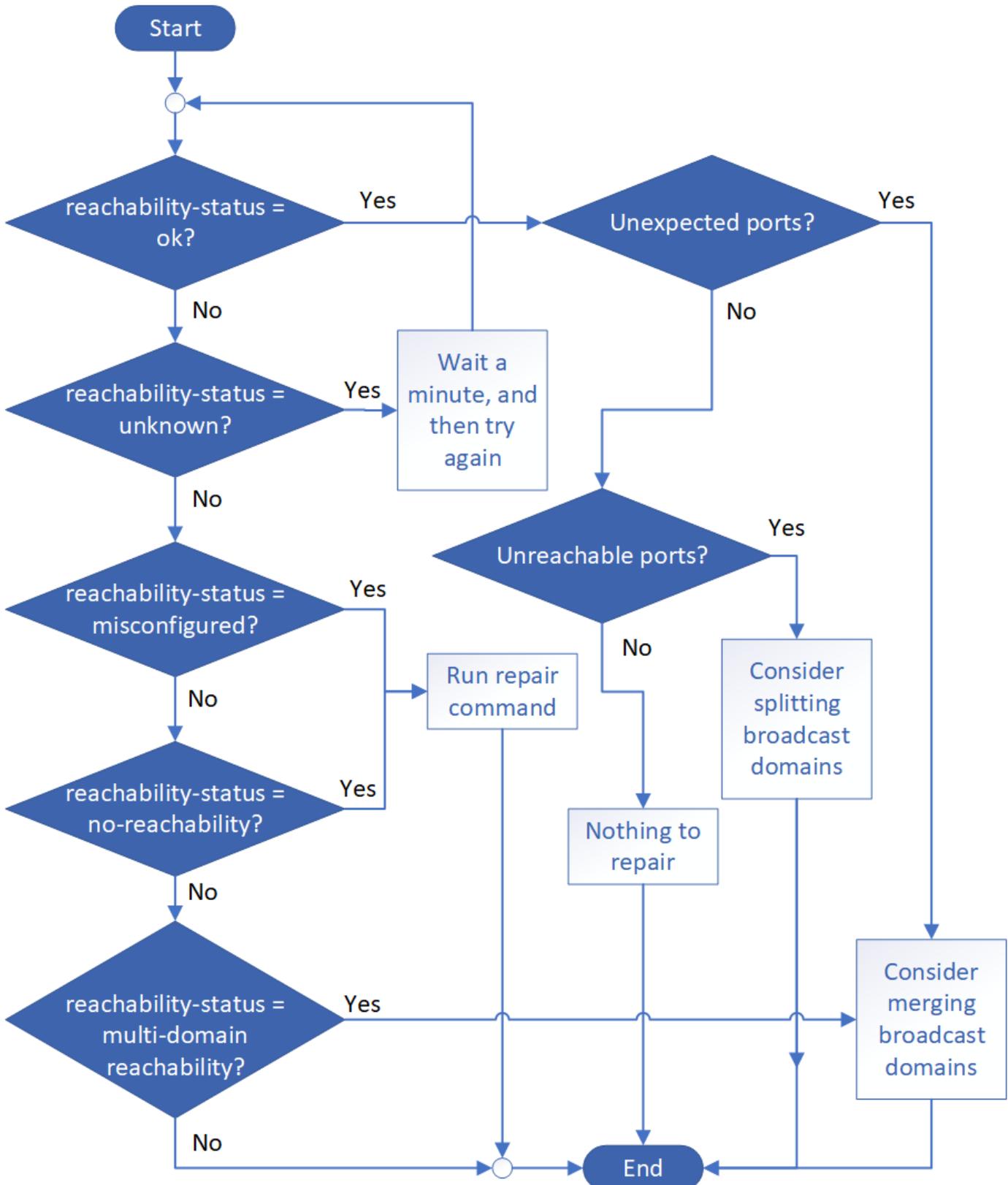
Use these commands to verify, diagnose, and repair network misconfigurations that stem from the ONTAP configuration not matching either the physical cabling or the network switch configuration.

Step

1. View port reachability:

```
network port reachability show
```

2. Use the following decision tree and table to determine the next step, if any.



Reachability-status	Description
ok	<p>The port has layer 2 reachability to its assigned broadcast domain.</p> <p>If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see the following <i>Unexpected ports</i> row.</p> <p>If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see the following <i>Unreachable ports</i> row.</p> <p>If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.</p>
Unexpected ports	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see Merge broadcast domains.</p>
Unreachable ports	<p>If a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology.</p> <p>Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain after you have verified that the physical and switch configuration is accurate.</p> <p>For more information, see Split broadcast domains.</p>
misconfigured-reachability	<p>The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability:</p> <pre>network port reachability repair -node -port</pre> <p>For more information, see Repair port reachability.</p>

Reachability-status	Description
no-reachability	<p>The port does not have layer 2 reachability to any existing broadcast domain.</p> <p>You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace:</p> <pre data-bbox="817 439 1503 502">network port reachability repair -node -port</pre> <p>For more information, see Repair port reachability.</p>
multi-domain-reachability	<p>The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain.</p> <p>Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains.</p> <p>For more information, see Merge broadcast domains or Repair port reachability.</p>
unknown	<p>If the reachability-status is "unknown", then wait a few minutes and try the command again.</p>

After you repair a port, you need to check for and resolve displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group. For more information, see [Repair port reachability](#).

Convert 40GbE NIC ports into multiple 10GbE ports for 10GbE connectivity

You can convert the X1144A-R6 and the X91440A-R6 40GbE Network Interface Cards (NICs) to support four 10GbE ports.

If you are connecting a hardware platform that supports one of these NICs to a cluster that supports 10GbE cluster interconnect and customer data connections, the NIC must be converted to provide the necessary 10GbE connections.

Before you begin

You must be using a supported breakout cable.

About this task

For a complete list of platforms that support NICs, see the [Hardware Universe](#).



On the X1144A-R6 NIC, only port A can be converted to support the four 10GbE connections. Once port A is converted, port e is not available for use.

Steps

1. Enter maintenance mode.
2. Convert the NIC from 40GbE support to 10GbE support.

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. After using the convert command, halt the node.
4. Install or change the cable.
5. Depending on the hardware model, use the SP (Service Processor) or BMC (Baseboard Management Controller) to power-cycle the node for the conversion to take effect.

Removing a NIC from the node on ONTAP 9.7 or earlier

This topic applies to ONTAP 9.7 or earlier. You might have to remove a faulty NIC from its slot or move the NIC to another slot for maintenance purposes.

Before you begin

- All LIFs hosted on the NIC ports must have been migrated or deleted.
- None of the NIC ports can be the home ports of any LIFs.
- You must have advanced privileges to delete the ports from a NIC.

Steps

1. Delete the ports from the NIC:

```
network port delete
```

2. Verify that the ports have been deleted:

```
network port show
```

3. Repeat step 1, if the output of the network port show command still shows the deleted port.

Removing a NIC from the node on ONTAP 9.8 or later

This topic applies to ONTAP 9.8 or later. You might have to remove a faulty NIC from its slot or move the NIC to another slot for maintenance purposes.

Steps

1. Power down the node.
2. Physically remove the NIC from its slot.
3. Power on the node.
4. Verify that the port has been deleted:

```
network port show
```



ONTAP automatically removes the port from any interface groups. If the port was the only member of an interface group, the interface group is deleted.

5. If the port had any VLANs configured on it, they are displaced. You can view displaced VLANs using the following command:

```
cluster controller-replacement network displaced-vlans show
```



The `displaced-interface show`, `displaced-vlans show`, and `displaced-vlans restore` commands are unique and do not require the fully qualified command name, which starts with `cluster controller-replacement network`.

6. These VLANs are deleted, but can be restored using the following command:

```
displaced-vlans restore
```

7. If the port had any LIFs configured on it, ONTAP automatically chooses new home ports for those LIFs on another port in the same broadcast domain. If no suitable home port is found on the same filer, those LIFs are considered displaced. You can view displaced LIFs using the following command:

```
displaced-interface show
```

8. When a new port is added to the broadcast domain on the same node, the home ports for the LIFs are automatically restored. Alternatively, you can either set the home port using `network interface modify -home-port -home-node` or use the `displaced-interface restore` command.

Configure IPspaces (cluster administrators only)

Overview

IPspaces enable you to configure a single ONTAP cluster so that it can be accessed by clients from more than one administratively separate network domain, even if those clients are using the same IP address subnet range. This allows for separation of client traffic for privacy and security.

An IPspace defines a distinct IP address space in which storage virtual machines (SVMs) reside. Ports and IP addresses defined for an IPspace are applicable only within that IPspace. A distinct routing table is maintained for each SVM within an IPspace; therefore, no cross-SVM or cross-IPspace traffic routing occurs.



IPspaces support both IPv4 and IPv6 addresses on their routing domains.

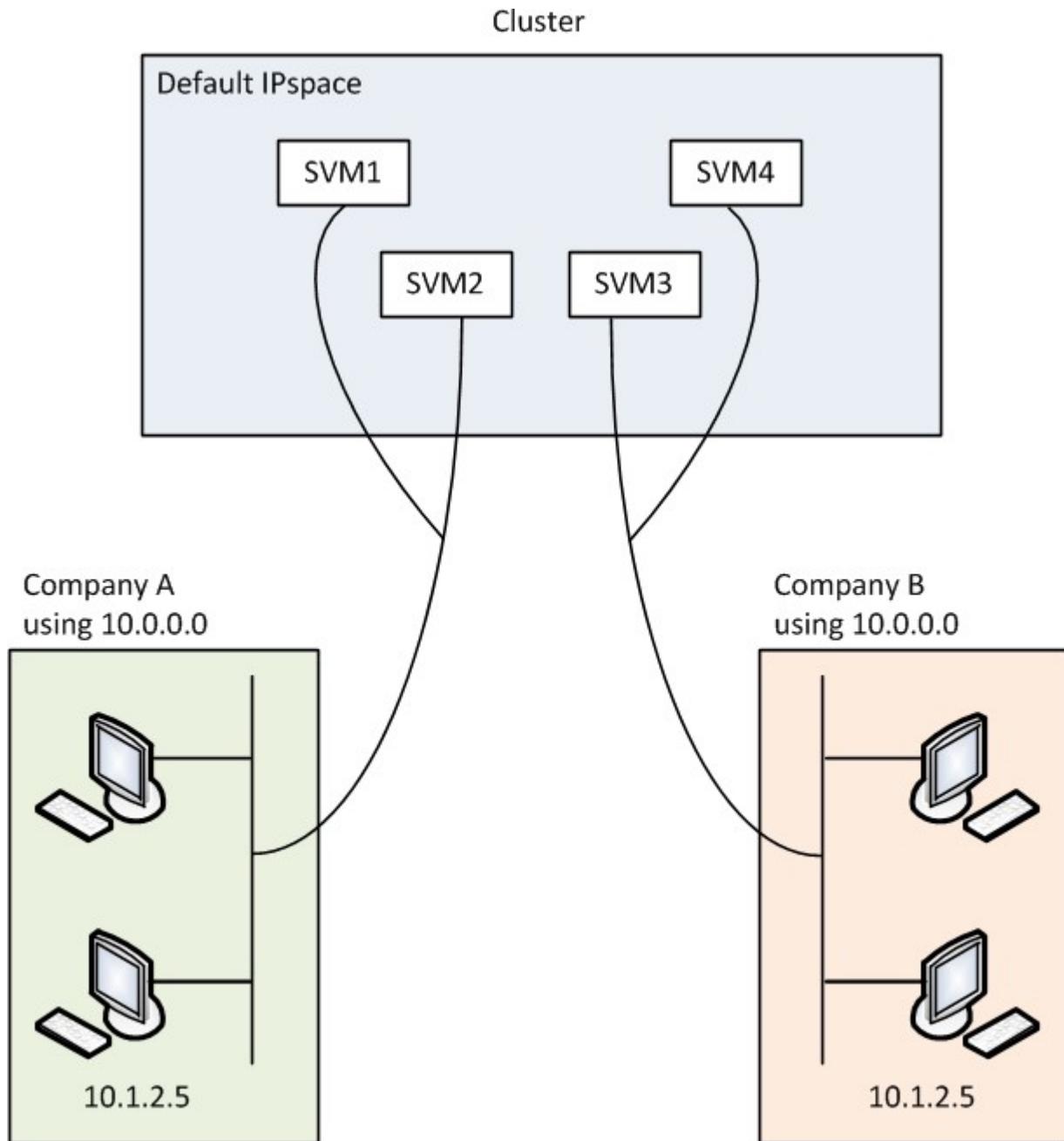
If you are managing storage for a single organization, then you do not need to configure IPspaces. If you are managing storage for multiple companies on a single ONTAP cluster, and you are certain that none of your customers have conflicting networking configurations, then you also do not need to use IPspaces. In many cases, the use of storage virtual machines (SVMs), with their own distinct IP routing tables, can be used to segregate unique networking configurations instead of using IPspaces.

Example of using IPspaces

A common application for using IPspaces is when a Storage Service Provider (SSP) needs to connect customers of companies A and B to an ONTAP cluster on the SSP's premises and both companies are using the same private IP address ranges.

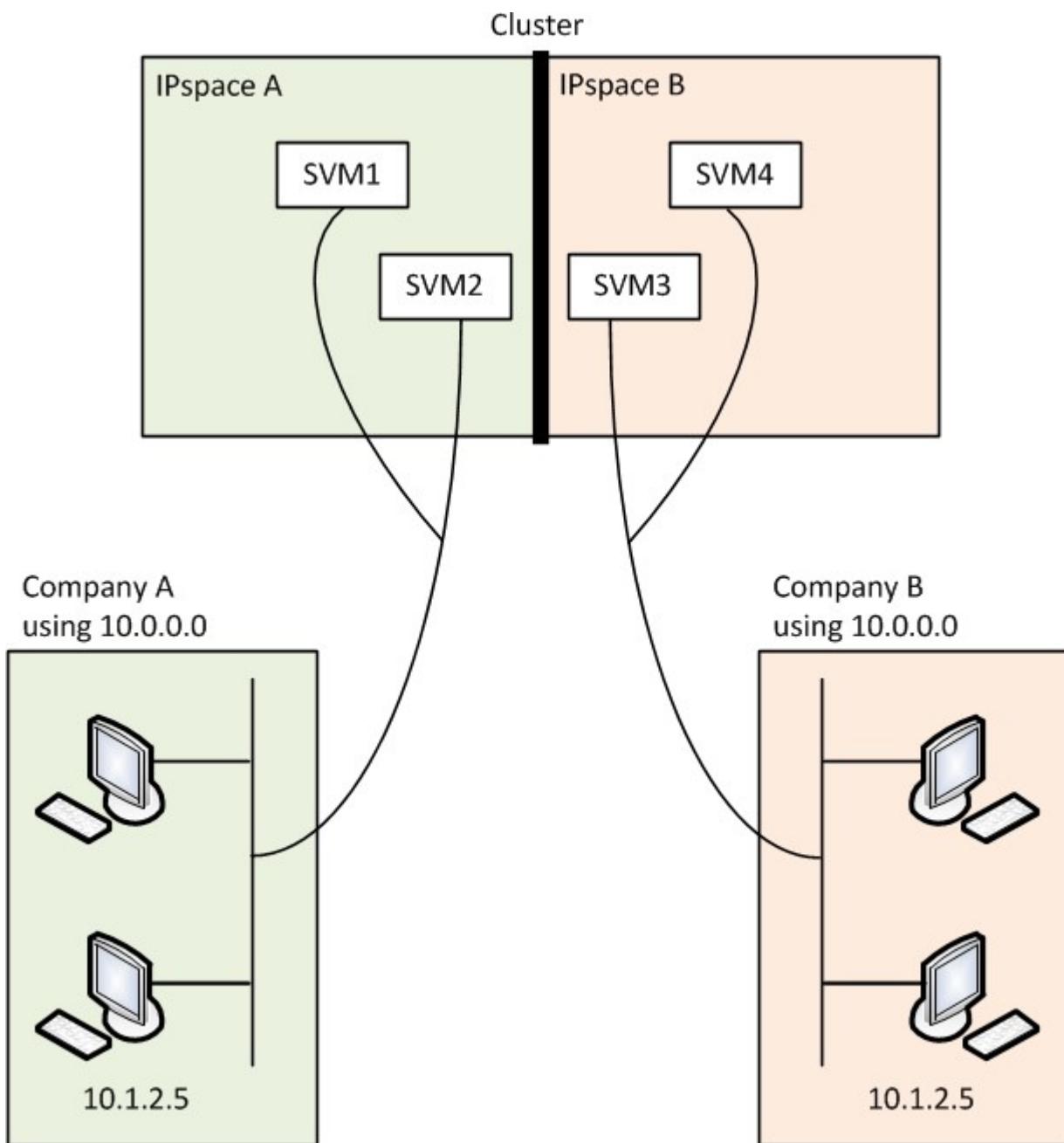
The SSP creates SVMs on the cluster for each customer and provides a dedicated network path from two SVMs to company A's network and from the other two SVMs to company B's network.

This type of deployment is shown in the following illustration, and it works if both companies use non-private IP address ranges. However, the illustration shows both companies using the same private IP address ranges, which causes problems.



Both companies use the private IP address subnet 10.0.0.0, causing the following problems:

- The SVMs in the cluster at the SSP location have conflicting IP addresses if both companies decide to use the same IP address for their respective SVMs.
- Even if the two companies agree on using different IP addresses for their SVMs, problems can arise.
- For example, if any client in A's network has the same IP address as a client in B's network, packets destined for a client in A's address space might get routed to a client in B's address space, and vice versa.
- If the two companies decide to use mutually exclusive address spaces (for example, A uses 10.0.0.0 with a network mask of 255.128.0.0 and B uses 10.128.0.0 with a network mask of 255.128.0.0), the SSP needs to configure static routes on the cluster to route traffic appropriately to A's and B's networks.
- This solution is neither scalable (because of static routes) nor secure (broadcast traffic is sent to all interfaces of the cluster). To overcome these problems, the SSP defines two IPspaces on the cluster—one for each company. Because no cross-IPspace traffic is routed, the data for each company is securely routed to its respective network even if all of the SVMs are configured in the 10.0.0.0 address space, as shown in the following illustration:



Additionally, the IP addresses referred to by the various configuration files, such as the `/etc/hosts` file, the `/etc/hosts.equiv` file, and `the /etc/rc` file, are relative to that IPspace. Therefore, the IPspaces enable the SSP to configure the same IP address for the configuration and authentication data for multiple SVMs, without conflict.

Standard properties of IPspaces

Special IPspaces are created by default when the cluster is first created. Additionally, special storage virtual machines (SVMs) are created for each IPspace.

Two IPspaces are created automatically when the cluster is initialized:

- "Default" IPspace

This IPspace is a container for ports, subnets, and SVMs that serve data. If your configuration does not need separate IPspaces for clients, all SVMs can be created in this IPspace. This IPspace also contains the cluster management and node management ports.

- "Cluster" IPspace

This IPspace contains all cluster ports from all nodes in the cluster. It is created automatically when the cluster is created. It provides connectivity to the internal private cluster network. As additional nodes join the cluster, cluster ports from those nodes are added to the "Cluster" IPspace.

A "system" SVM exists for each IPspace. When you create an IPspace, a default system SVM of the same name is created:

- The system SVM for the "Cluster" IPspace carries cluster traffic between nodes of a cluster on the internal private cluster network.

It is managed by the cluster administrator, and it has the name "Cluster".

- The system SVM for the "Default" IPspace carries management traffic for the cluster and nodes, including the intercluster traffic between clusters.

It is managed by the cluster administrator, and it uses the same name as the cluster.

- The system SVM for a custom IPspace that you create carries management traffic for that SVM.

It is managed by the cluster administrator, and it uses the same name as the IPspace.

One or more SVMs for clients can exist in an IPspace. Each client SVM has its own data volumes and configurations, and it is administered independently of other SVMs.

Create IPspaces

IPspaces are distinct IP address spaces in which storage virtual machines (SVMs) reside. You can create IPspaces when you need your SVMs to have their own secure storage, administration, and routing.

About this task

There is a cluster-wide limit of 512 IPspaces. The cluster-wide limit is reduced to 256 IPspaces for clusters that contain nodes with 6 GB of RAM or less for platforms such as FAS2220 or FAS2240. See the Hardware

Universe to determine whether additional limits apply to your platform.

NetApp Hardware Universe



An IPspace name cannot be "all" because "all" is a system-reserved name.

Step

Create an IPspace:

```
network ipspace create -ipspace ipspace_name
```

ipspace_name is the name of the IPspace that you want to create. The following command creates the IPspace *ipspace1* on a cluster:

```
network ipspace create -ipspace ipspace1
```

After you finish

If you create an IPspace in a cluster with a MetroCluster configuration, IPspace objects must be manually replicated to the partner clusters. Any SVMs that are created and assigned to an IPspace before the IPspace is replicated will not be replicated to the partner clusters.

Broadcast domains are created automatically in the "Default" IPspace and can be moved between IPspaces using the following command:

```
network port broadcast-domain move
```

For example, if you want to move a broadcast domain from "Default" to "ips1", using the following command:

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default -to-ipspace ips1
```

Display IPspaces

You can display the list of IPspaces that exist in a cluster, and you can view the storage virtual machines (SVMs), broadcast domains, and ports that are assigned to each IPspace.

Step

Display the IPspaces and SVMs in a cluster:

```
network ipspace show [-ipspace ipspace_name]
```

The following command displays all of the IPspaces, SVMs, and broadcast domains in the cluster:

```

network ipspace show
IPspace          Vserver List           Broadcast Domains
-----  -----  -----
Cluster          Cluster             Cluster
Default          vs1, cluster-1        Default
ipspace1         vs3, vs4, ipspace1   bcast1

```

The following command displays the nodes and ports that are part of IPspace ipspace1:

```

network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1

```

Delete an IPspace

If you no longer need an IPspace, you can delete it.

Before you begin

There must be no broadcast domains, network interfaces, or SVMs associated with the IPspace you want to delete.

The system-defined "Default" and "Cluster" IPspaces cannot be deleted.

Step

Delete an IPspace:

```
network ipspace delete -ipspace ipspace_name
```

The following command deletes IPspace ipspace1 from the cluster:

```
network ipspace delete -ipspace ipspace1
```

ONTAP 9.8 and later-Configure broadcast domains (cluster administrators only)

Overview for ONTAP 9.8 and later

Broadcast domains are intended to group network ports that belong to the same layer 2

network. The ports in the group can then be used by a storage virtual machine (SVM) for data or management traffic.

A broadcast domain resides in an IPspace. During cluster initialization, the system creates two default broadcast domains:

- The "Default" broadcast domain contains ports that are in the "Default" IPspace.

These ports are used primarily to serve data. Cluster management and node management ports are also in this broadcast domain.

- The "Cluster" broadcast domain contains ports that are in the "Cluster" IPspace.

These ports are used for cluster communication and include all cluster ports from all nodes in the cluster.

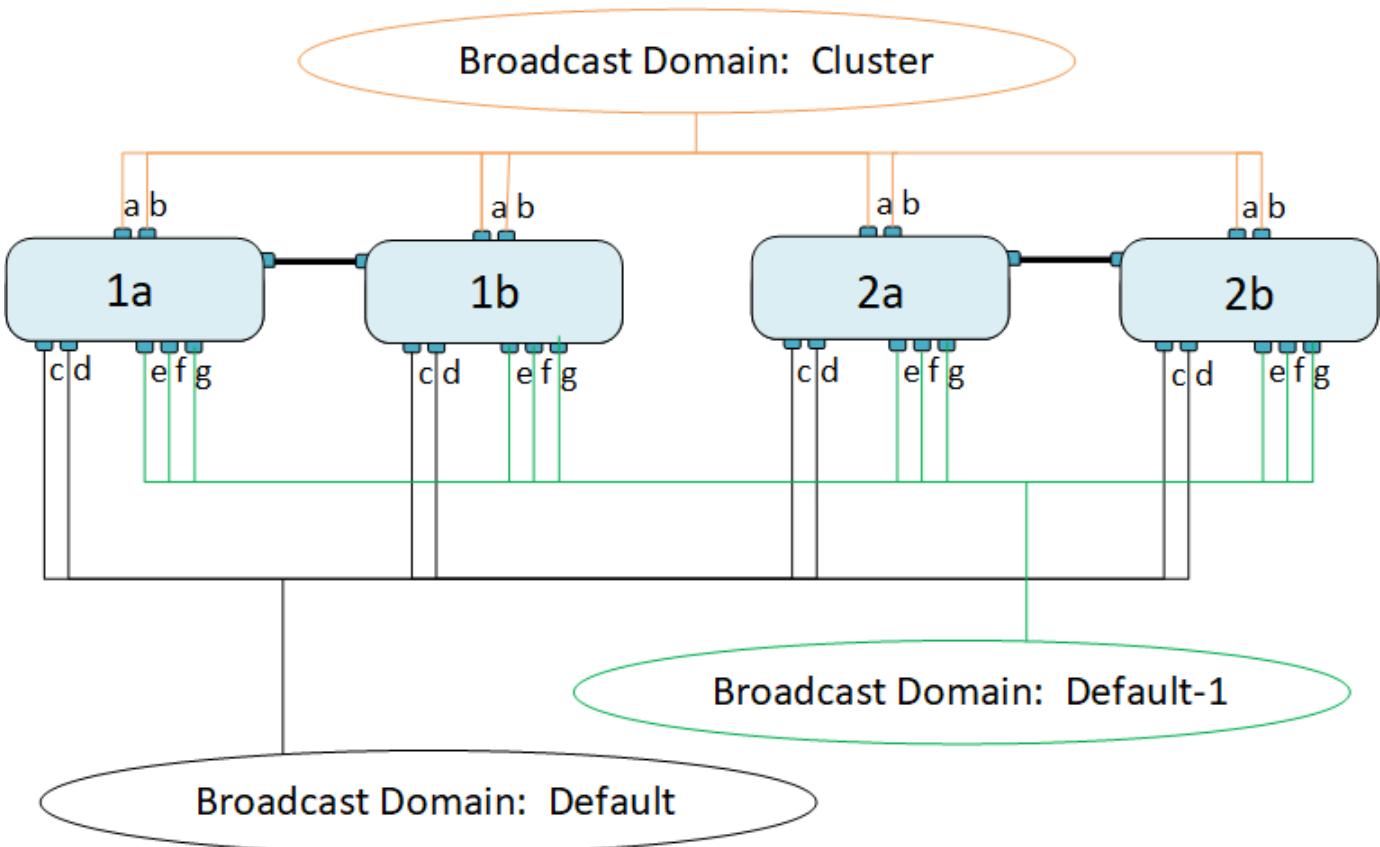
The system creates additional broadcast domains in the Default IPspace when necessary. The "Default" broadcast domain contains the home-port of the management LIF, plus any other ports that have layer 2 reachability to that port. Additional broadcast domains are named "Default-1", "Default-2", and so forth.

Example of using broadcast domains

A broadcast domain is a set of network ports in the same IPspace that also has layer 2 reachability to one another, typically including ports from many nodes in the cluster.

The illustration shows the ports assigned to three broadcast domains in a four-node cluster:

- The "Cluster" broadcast domain is created automatically during cluster initialization, and it contains ports a and b from each node in the cluster.
- The "Default" broadcast domain is also created automatically during cluster initialization, and it contains ports c and d from each node in the cluster.
- The system automatically creates any additional broadcast domains during cluster initialization based on layer 2 network reachability. These additional broadcast domains are named Default-1, Default-2, and so forth.



A failover group of the same name and with the same network ports as each of the broadcast domains is created automatically. This failover group is automatically managed by the system, meaning that as ports are added or removed from the broadcast domain, they are automatically added or removed from this failover group.

Add or remove ports from a broadcast domain

Broadcast domains are automatically created during the cluster create or join operation. You do not need to manually remove ports from broadcast domains.

If network port reachability has changed, either through physical network connectivity or switch configuration, and a network port belongs in a different broadcast domain, see the following topic:

[Repair port reachability](#)

Split broadcast domains

If network port reachability has changed, either through physical network connectivity or switch configuration, and a group of network ports previously configured in a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology.

To determine if a network port broadcast domain is partitioned into more than one reachability set, use the `network port reachability show -details` command and pay attention to which ports do not have connectivity to one another ("Unreachable ports"). Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain, after you have verified that the physical and switch

configuration is accurate.

Step

Split a broadcast domain into two broadcast domains:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port, node:port>
```

- `ipspace_name` is the name of the ipspace where the broadcast domain resides.
- `-broadcast-domain` is the name of the broadcast domain that will be split.
- `-new-broadcast-domain` is the name of the new broadcast domain that will be created.
- `-ports` is the node name and port to be added to the new broadcast domain.

Merge broadcast domains

If network port reachability has changed, either through physical network connectivity or switch configuration, and two group of network ports previously configured in multiple broadcast domains now all share reachability, then merging two broadcast domains can be used to synchronize the ONTAP configuration with the physical network topology.

To determine if multiple broadcast domains belong to one reachability set, use the "network port reachability show -details" command and pay attention to which ports that are configured in another broadcast domain actually have connectivity to one another ("Unexpected ports"). Typically, the list of unexpected ports defines the set of ports that should be merged into the broadcast domain after you have verified that the physical and switch configuration is accurate.

Step

Merge the ports from one broadcast domain into an existing broadcast domain:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` is the name of the ipspace where the broadcast domains reside.
- `-broadcast-domain` is the name of the broadcast domain that will be merged.
- `-into-broadcast-domain` is the name of the broadcast domain that will receive additional ports.

Change the MTU value for ports in a broadcast domain

You can modify the MTU value for a broadcast domain to change the MTU value for all ports in that broadcast domain. This can be done to support topology changes that have been made in the network.

Before you begin

The MTU value must match all the devices connected to that layer 2 network except for the e0M port handling management traffic.

About this task

Changing the MTU value causes a brief interruption in traffic over the affected ports. The system displays a prompt that you must answer with y to make the MTU change.

Step

Change the MTU value for all ports in a broadcast domain:

```
network port broadcast-domain modify -broadcast-domain  
<broadcast_domain_name> -mtu <mtu_valu> [-ipspace <ipspace_name>]
```

- `broadcast_domain` is the name of the broadcast domain.
- `mtu` is the MTU size for IP packets; 1500 and 9000 are typical values.
- `ipspace` is the name of the IPspace in which this broadcast domain resides. The "Default" IPspace is used unless you specify a value for this option. The following command changes the MTU to 9000 for all ports in the broadcast domain bcast1:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <9000>  
Warning: Changing broadcast domain settings will cause a momentary data-serving interruption.  
Do you want to continue? {y|n}: <y>
```

Display broadcast domains

You can display the list of broadcast domains within each IPspace in a cluster. The output also shows the list of ports and the MTU value for each broadcast domain.

Step

Display the broadcast domains and associated ports in the cluster:

```
network port broadcast-domain show
```

The following command displays all the broadcast domains and associated ports in the cluster:

network port broadcast-domain show				Update
IPspace Broadcast				Status Details
Name	Domain Name	MTU	Port List	
<hr/>				
Cluster	Cluster	9000	cluster-1-01:e0a cluster-1-01:e0b cluster-1-02:e0a cluster-1-02:e0b	complete complete complete complete
Default	Default	1500	cluster-1-01:e0c cluster-1-01:e0d cluster-1-02:e0c cluster-1-02:e0d	complete complete complete complete
	Default-1	1500	cluster-1-01:e0e cluster-1-01:e0f cluster-1-01:e0g cluster-1-02:e0e cluster-1-02:e0f cluster-1-02:e0g	complete complete complete complete complete complete

The following command displays the ports in the Default-1 broadcast domain that have an update status of error, which indicate that the port could not be updated properly:

network port broadcast-domain show -broadcast-domain Default-1 -port -update-status error				Update
IPspace Broadcast				Status Details
Name	Domain Name	MTU	Port List	
<hr/>				
Default	Default-1	1500	cluster-1-02:e0g	error

For more information, see [ONTAP 9 commands](#).

Delete a broadcast domain

If you no longer need a broadcast domain, you can delete it. This moves the ports associated with that broadcast domain to the "Default" IPspace.

Before you begin

There must be no subnets, network interfaces, or SVMs associated with the broadcast domain you want to delete.

About this task

- The system-created "Cluster" broadcast domain cannot be deleted.
- All failover groups related to the broadcast domain are removed when you delete the broadcast domain.

Step

Delete a broadcast domain:

```
network port broadcast-domain delete -broadcast-domain  
<broadcast_domain_name> [-ipspace <ipspace_name>]
```

The following command deletes broadcast domain Default-1 in IPspace ipspace1:

```
network port broadcast-domain delete -broadcast-domain <Default-1>  
-ipspace <ipspace1>
```

ONTAP 9.7 and earlier-Configure broadcast domains (cluster administrators only)

Overview for ONTAP 9.7 and earlier

Broadcast domains are intended to group network ports that belong to the same layer 2 network. The ports in the group can then be used by a storage virtual machine (SVM) for data or management traffic.

A broadcast domain resides in an IPspace. During cluster initialization, the system creates two default broadcast domains:

- The Default broadcast domain contains ports that are in the Default IPspace.
These ports are used primarily to serve data. Cluster management and node management ports are also in this broadcast domain.
- The Cluster broadcast domain contains ports that are in the Cluster IPspace.
These ports are used for cluster communication and include all cluster ports from all nodes in the cluster.

If you have created unique IPspaces to separate client traffic, then you need to create a broadcast domain in each of those IPspaces.



Create a broadcast domain to group network ports in the cluster that belong to the same layer 2 network. The ports can then be used by SVMs.

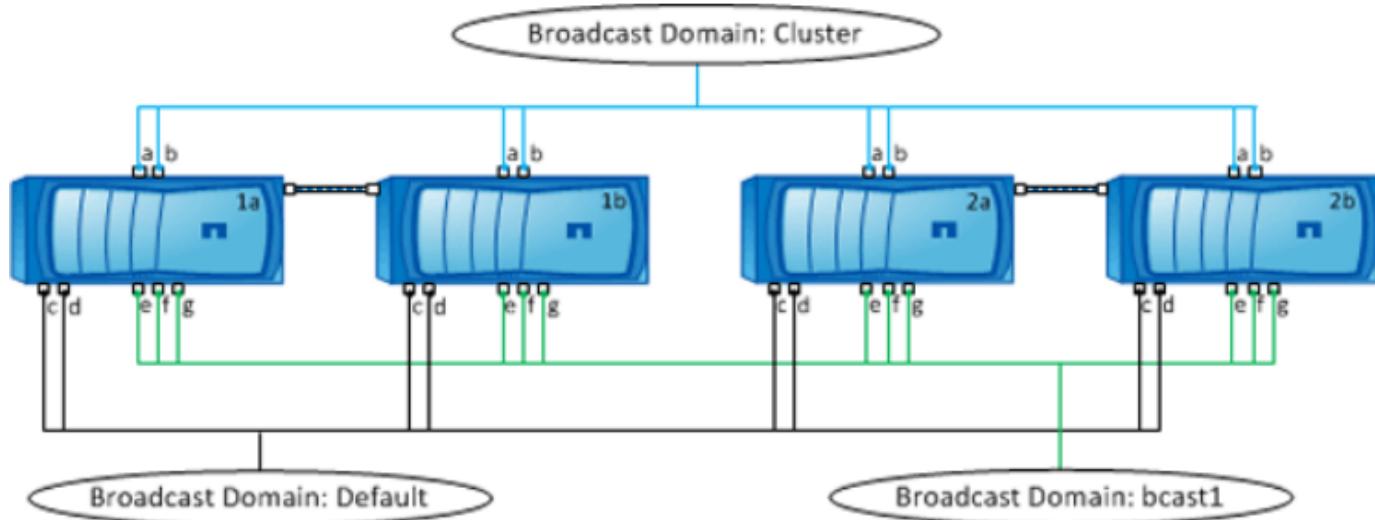
Example of using broadcast domains

A broadcast domain is a set of network ports in the same IPspace that also has layer 2 reachability to one another, typically including ports from many nodes in the cluster.

The illustration shows the ports assigned to three broadcast domains in a four-node cluster:

- The Cluster broadcast domain is created automatically during cluster initialization, and it contains ports a and b from each node in the cluster.

- The Default broadcast domain is also created automatically during cluster initialization, and it contains ports c and d from each node in the cluster.
 - The bcast1 broadcast domain has been created manually, and it contains ports e, f, and g from each node in the cluster.
- This broadcast domain was created by the system administrator specifically for a new client to access data through a new SVM.



A failover group of the same name and with the same network ports as each of the broadcast domains is created automatically. This failover group is automatically managed by the system, meaning that as ports are added or removed from the broadcast domain, they are automatically added or removed from this failover group.

Create a broadcast domain

In ONTAP 9.7 and earlier, you create a broadcast domain to group network ports in the cluster that belong to the same layer 2 network. The ports can then be used by SVMs.

Before you begin

Starting with ONTAP 9.8, broadcast domains are automatically created during the cluster create or join operation. If you are running ONTAP 9.8 or later, these steps are not needed.

In ONTAP 9.7 and earlier, the ports you plan to add to the broadcast domain must not belong to another broadcast domain.

About this task

- All broadcast domain names must be unique within an IPspace.
- The ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).
- If the ports you want to use belong to another broadcast domain, but are unused, you use the `network port broadcast-domain remove-ports` command to remove the ports from the existing broadcast domain.
- The MTU of the ports added to a broadcast domain are updated to the MTU value set in the broadcast domain.
- The MTU value must match all of the devices connected to that layer 2 network except for the e0M port handling management traffic.

- If you do not specify an IPspace name, the broadcast domain is created in the "Default" IPspace.

To make system configuration easier, a failover group of the same name is created automatically that contains the same ports.

Steps

1. View the ports that are not currently assigned to a broadcast domain:

```
network port show
```

If the display is large, use the `network port show -broadcast-domain` command to view only unassigned ports.

2. Create a broadcast domain:

```
network port broadcast-domain create -broadcast-domain broadcast_domain_name
-mtu mtu_value [-ipspace ipspace_name] [-ports ports_list]
```

- `broadcast_domain_name` is the name of the broadcast domain you want to create.
- `mtu_value` is the MTU size for IP packets; 1500 and 9000 are typical values.

This value is applied to all ports that are added to this broadcast domain.

- `ipspace_name` is the name of the IPspace to which this broadcast domain will be added.

The "Default" IPspace is used unless you specify a value for this parameter.

- `ports_list` is the list of ports that will be added to the broadcast domain.

The ports are added in the format `node_name:port_number`, for example, `node1:e0c`.

3. Verify that the broadcast domain was created as desired:

```
network port show -instance -broadcast-domain new_domain
```

Example

The following command creates broadcast domain `bcast1` in the Default IPspace, sets the MTU to 1500, and adds four ports:

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

After you finish

You can define the pool of IP addresses that will be available in the broadcast domain by creating a subnet, or you can assign SVMs and interfaces to the IPspace at this time. For more information, see the [Cluster and SVM Peering Express Guide](#).

If you need to change the name of an existing broadcast domain, you use the `network port broadcast-domain rename` command.

Add or remove ports from a broadcast domain

You can add network ports when initially creating a broadcast domain, or you can add

ports to, or remove ports from, a broadcast domain that already exists. This allows you to efficiently use all the ports in the cluster.

Before you begin

- Ports you plan to add to a broadcast domain must not belong to another broadcast domain.
- Ports that already belong to an interface group cannot be added individually to a broadcast domain.

About this task

The following rules apply when adding and removing network ports:

When adding ports...	When removing ports...
The ports can be network ports, VLANs, or interface groups (ifgrps).	N/A
The ports are added to the system-defined failover group of the broadcast domain.	The ports are removed from all failover groups in the broadcast domain.
The MTU of the ports is updated to the MTU value set in the broadcast domain.	The MTU of the ports is unchanged.
The IPspace of the ports is updated to the IPspace value of the broadcast domain.	The ports are moved to the 'Default' IPspace with no broadcast domain attribute.



If you remove the last member port of an interface group using the `network port ifgrp remove-port` command, it causes the interface group port to be removed from the broadcast domain because an empty interface group port is not allowed in a broadcast domain.

Steps

- Display the ports that are currently assigned or unassigned to a broadcast domain by using the `network port show` command.
- Add or remove network ports from the broadcast domain:

If you want to...	Use...
Add ports to a broadcast domain	<code>network port broadcast-domain add-ports</code>
Remove ports from a broadcast domain	<code>network port broadcast-domain remove-ports</code>

For more information about these commands, see [ONTAP 9 commands](#).

Examples of adding and removing ports

The following command adds port e0g on node cluster-1-01 and port e0g on node cluster-1-02 to broadcast domain bcast1 in the Default IPspace:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0g,cluster1-02:e0g
```

The following command adds two cluster ports to broadcast domain Cluster in the Cluster IPspace:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster  
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

The following command removes port e0e on node cluster1-01 from broadcast domain bcast1 in the Default IPspace:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1  
-ports cluster-1-01:e0e
```

Split broadcast domains

You can modify an existing broadcast domain by splitting it into two different broadcast domains, with each broadcast domain containing some of the original ports assigned to the original broadcast domain.

About this task

- If the ports are in a failover group, all of the ports in a failover group must be split.
- If the ports have LIFs associated with them, the LIFs cannot be part of a subnet's ranges.

Step

Split a broadcast domain into two broadcast domains:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast  
-domain <broadcast_domain_name> -new-broadcast-domain  
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` is the name of the IPspace where the broadcast domain resides.
- `-broadcast-domain` is the name of the broadcast domain that will be split.
- `-new-broadcast-domain` is the name of the new broadcast domain that will be created.
- `-ports` is the node name and port to be added to the new broadcast domain.

Merge broadcast domains

You can move all of the ports from one broadcast domain into an existing broadcast domain using the merge command.

This operation reduces the steps required if you were to remove all ports from a broadcast domain and then add the ports to an existing broadcast domain.

Step

Merge the ports from one broadcast domain into an existing broadcast domain:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- **ipspace_name** is the name of the IPspace where the broadcast domains reside.
- **-broadcast-domain** is the name of the broadcast domain that will be merged.
- **-into-broadcast-domain** is the name of the broadcast domain that will receive additional ports.

Example

The following example merges broadcast domain bd-data1 into broadcast domain bd-data2:

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

Change the MTU value for ports in a broadcast domain

You can modify the MTU value for a broadcast domain to change the MTU value for all ports in that broadcast domain. This can be done to support topology changes that have been made in the network.

Before you begin

The MTU value must match all the devices connected to that layer 2 network except for the e0M port handling management traffic.

About this task

Changing the MTU value causes a brief interruption in traffic over the affected ports. The system displays a prompt that you must answer with y to make the MTU change.

Step

Change the MTU value for all ports in a broadcast domain:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_valu> [-ipspace <ipspace_name>]
```

- **broadcast_domain** is the name of the broadcast domain.
- **mtu** is the MTU size for IP packets; 1500 and 9000 are typical values.
- **ipspace** is the name of the IPspace in which this broadcast domain resides. The "Default" IPspace is used unless you specify a value for this option. The following command changes the MTU to 9000 for all ports in the broadcast domain bcast1:

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <9000>
Warning: Changing broadcast domain settings will cause a momentary data-serving interruption.
Do you want to continue? {y|n}: <y>
```

Display broadcast domains

You can display the list of broadcast domains within each IPspace in a cluster. The output also shows the list of ports and the MTU value for each broadcast domain.

Step

Display the broadcast domains and associated ports in the cluster:

```
network port broadcast-domain show
```

The following command displays all the broadcast domains and associated ports in the cluster:

network port broadcast-domain show				Update	
IPspace	Broadcast	Name	MTU	Port List	Status Details
Cluster	Cluster	Cluster	9000	cluster-1-01:e0a cluster-1-01:e0b cluster-1-02:e0a cluster-1-02:e0b	complete complete complete complete
Default	Default	bcast1	1500	cluster-1-01:e0c cluster-1-01:e0d cluster-1-02:e0c cluster-1-02:e0d	complete complete complete complete
			1500	cluster-1-01:e0e cluster-1-01:e0f cluster-1-01:e0g cluster-1-02:e0e cluster-1-02:e0f cluster-1-02:e0g	complete complete complete complete complete complete

The following command displays the ports in the bcast1 broadcast domain that have an update status of error, which indicate that the port could not be updated properly:

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update  
-status error
```

IPspace Broadcast				Update
Name	Domain Name	MTU	Port List	Status Details
Default	bcast1	1500	cluster-1-02:e0g	error

For more information, see [ONTAP 9 commands](#).

Delete a broadcast domain

If you no longer need a broadcast domain, you can delete it. This moves the ports associated with that broadcast domain to the "Default" IPspace.

Before you begin

There must be no subnets, network interfaces, or SVMs associated with the broadcast domain you want to delete.

About this task

- The system-created "Cluster" broadcast domain cannot be deleted.
- All failover groups related to the broadcast domain are removed when you delete the broadcast domain.

Step

Delete a broadcast domain:

```
network port broadcast-domain delete -broadcast-domain  
<broadcast_domain_name> [-ipspace <ipspace_name>]
```

The following command deletes broadcast domain bcast1 in IPspace ipspace1:

```
network port broadcast-domain delete -broadcast-domain <bcast1> -ipspace  
<ipspace1>
```

Configure failover groups and policies for LIFs

Overview

LIF failover refers to the automatic migration of a LIF to a different network port in response to a link failure on the LIF's current port. This is a key component to providing high availability for the connections to SVMs. Configuring LIF failover involves creating a failover group, modifying the LIF to use the failover group, and specifying a failover policy.

A failover group contains a set of network ports (physical ports, VLANs, and interface groups) from one or

more nodes in a cluster. The network ports that are present in the failover group define the failover targets available for the LIF. A failover group can have cluster management, node management, intercluster, and NAS data LIFs assigned to it.



When a LIF is configured without a valid failover target, an outage occurs when the LIF attempts to fail over. You can use the "network interface show -failover" command to verify the failover configuration.

When you create a broadcast domain, a failover group of the same name is created automatically that contains the same network ports. This failover group is automatically managed by the system, meaning that as ports are added or removed from the broadcast domain, they are automatically added or removed from this failover group. This is provided as an efficiency for administrators who do not want to manage their own failover groups.

Create a failover group

You create a failover group of network ports so that a LIF can automatically migrate to a different port if a link failure occurs on the LIF's current port. This enables the system to reroute network traffic to other available ports in the cluster.

About this task

You use the `network interface failover-groups create` command to create the group and to add ports to the group.

- The ports added to a failover group can be network ports, VLANs, or interface groups (ifgrps).
- All the ports added to the failover group must belong to the same broadcast domain.
- A single port can reside in multiple failover groups.
- If you have LIFs in different VLANs or broadcast domains, you must configure failover groups for each VLAN or broadcast domain.
- Failover groups do not apply in SAN iSCSI or FC environments.

Step

Create a failover group:

```
network interface failover-groups create -vserver vserver_name -failover-group failover_group_name -targets ports_list
```

- `vserver_name` is the name of the SVM that can use the failover group.
- `failover_group_name` is the name of the failover group you want to create.
- `ports_list` is the list of ports that will be added to the failover group.
Ports are added in the format `node_name:<port_number>`, for example, `node1:e0c`.

The following command creates failover group fg3 for SVM vs3 and adds two ports:

```
network interface failover-groups create -vserver vs3 -failover-group fg3 -targets cluster1-01:e0e,cluster1-02:e0e
```

After you finish

- You should apply the failover group to a LIF now that the failover group has been created.
- Applying a failover group that does not provide a valid failover target for a LIF results in a warning message.

If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

Configure failover settings on a LIF

You can configure a LIF to fail over to a specific group of network ports by applying a failover policy and a failover group to the LIF. You can also disable a LIF from failing over to another port.

About this task

- When a LIF is created, LIF failover is enabled by default, and the list of available target ports is determined by the default failover group and failover policy based on the LIF type and service policy.

Starting with 9.5, you can specify a service policy for the LIF that defines which network services can use the LIF. Some network services impose failover restrictions on a LIF.



If a LIF's service policy is changed in a way that further restricts failover, the LIF's failover policy is automatically updated by the system.

- You can modify the failover behavior of LIFs by specifying values for the -failover-group and -failover-policy parameters in the network interface modify command.
- Modification of a LIF that results in the LIF having no valid failover target results in a warning message.

If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

- The following list describes how the -failover-policy setting affects the target ports that are selected from the failover group:

- **broadcast-domain-wide** applies to all ports on all nodes in the failover group.
- **system-defined** applies to only those ports on the LIF's home node and one other node in the cluster, typically a non-SFO partner, if it exists.
- **local-only** applies to only those ports on the LIF's home node.
- **sfo-partner-only** applies to only those ports on the LIF's home node and its SFO partner.
- **disabled** indicates the LIF is not configured for failover.



Logical interfaces for SAN protocols do not support failover, therefore, these LIFs are always set to disabled.

Step

Configure failover settings for an existing interface:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover  
-policy <failover_policy> -failover-group <failover_group>
```

Examples of configuring failover settings and disabling failover

The following command sets the failover policy to broadcast-domain-wide and uses the ports in failover group fg3 as failover targets for LIF data1 on SVM vs3:

```
network interface modify -vserver vs3 -lif data1 failover-policy
broadcast-domain-wide - failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif          failover-policy      failover-group
-----  -----  -----
vs3      data1      broadcast-domain-wide  fg3
```

The following command disables failover for LIF data1 on SVM vs3:

```
network interface modify -vserver vs3 -lif data1 failover-policy disabled
```

Commands for managing failover groups and policies

You can use the `network interface failover-groups` commands to manage failover groups. You use the `network interface modify` command to manage the failover groups and failover policies that are applied to a LIF.

If you want to...	Use this command...
Add network ports to a failover group	<code>network interface failover-groups add-targets</code>
Remove network ports from a failover group	<code>network interface failover-groups remove-targets</code>
Modify network ports in a failover group	<code>network interface failover-groups modify</code>
Display the current failover groups	<code>network interface failover-groups show</code>
Configure failover on a LIF	<code>network interface modify -failover-group -failover-policy</code>
Display the failover group and failover policy that is being used by each LIF	<code>network interface show -fields failover-group, failover-policy</code>
Rename a failover group	<code>network interface failover-groups rename</code>
Delete a failover group	<code>network interface failover-groups delete</code>



Modifying a failover group such that it does not provide a valid failover target for any LIF in the cluster can result in an outage when a LIF attempts to fail over.

For more information, see the man pages for the `network interface failover-groups` and `network interface modify` commands.

Configure subnets (cluster administrators only)

Overview

Subnets enable you to allocate specific blocks, or pools, of IP addresses for your ONTAP network configuration. This enables you to create LIFs more easily when using the `network interface create` command, by specifying a subnet name instead of having to specify IP address and network mask values.

A subnet is created within a broadcast domain, and it contains a pool of IP addresses that belong to the same layer 3 subnet. IP addresses in a subnet are allocated to ports in the broadcast domain when LIFs are created. When LIFs are removed, the IP addresses are returned to the subnet pool and are available for future LIFs.

It is recommended that you use subnets because they make the management of IP addresses much easier, and they make the creation of LIFs a simpler process. Additionally, if you specify a gateway when defining a subnet, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.

Create a subnet

After you create the broadcast domain, you can create a subnet to allocate specific blocks of IPv4 or IPv6 addresses to be used later when you create LIFs for the SVM.

This enables you to create LIFs more easily by specifying a subnet name instead of having to specify IP address and network mask values for each LIF.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Create a subnet.

```
network subnet create -broadcast-domain ipspace1 -ipspace ipspace1  
-subnet-name ipspace1 -subnet 10.0.0.0/24 -gateway 10.0.0.1 -ip-ranges  
"10.0.0.128-10.0.0.130,10.0.0.132"
```

The subnet name can be either a subnet IP value such as `192.0.2.0/24` or a string such as `ipspace1` like the one used in this example.

2. Verify that the subnet configuration is correct.

The output from this example shows information about the subnet named `ipspace1` in the `ipspace1` IPspace. The subnet belongs to the broadcast domain name `ipspace1`. You can assign the IP addresses in this subnet to data LIFs for SVMs created in the `ipspace1` IPspace.

```
network subnet show -ipspace ipspace1
```

Add or remove IP addresses from a subnet

You can add IP addresses when initially creating a subnet, or you can add IP addresses

to a subnet that already exists. You can also remove IP addresses from an existing subnet. This enables you to allocate only the required IP addresses for SVMs.

About this task

When adding IP addresses, you will receive an error if any service processor or network interfaces are using the IP addresses in the range being added. If you want to associate any manually addressed interfaces with the current subnet, you can set the "-force-update-lif-associations" option to true.

When removing IP addresses, you will receive an error if any service processor or network interfaces are using the IP addresses being removed. If you want the interfaces to continue to use the IP addresses after they are removed from the subnet, you can set the "-force-update-lif-associations" option to true.

Step

Add or remove IP addresses from a subnet:

If you want to...	Use this command...
Add IP addresses to a subnet	network subnet add-ranges
Remove IP addresses from a subnet	network subnet remove-ranges

For more information about these commands, see the man pages.

The following command adds IP addresses 192.0.2.82 through 192.0.2.85 to subnet sub1:

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

The following command removes IP address 198.51.100.9 from subnet sub3:

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges <198.51.100.9>
```

If the current range includes 1 through 10 and 20 through 40, and you want to add 11 through 19 and 41 through 50 (basically allowing 1 through 50), you can overlap the existing range of addresses by using the following command. This command adds only the new addresses and does not affect the existing addresses:

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-198.51.10.50>
```

Change subnet properties

You can change the subnet address and mask value, gateway address, or range of IP addresses in an existing subnet.

About this task

- When modifying IP addresses, you must ensure there are no overlapping IP addresses in the network so

that different subnets, or hosts, do not attempt to use the same IP address.

- If you add or change the gateway IP address, the modified gateway is applied to new SVMs when a LIF is created in them using the subnet. A default route to the gateway is created for the SVM if the route does not already exist. You may need to manually add a new route to the SVM when you change the gateway IP address.

Step

Modify subnet properties:

```
network subnet modify -subnet-name <subnet_name> [-ipspace <ipspace_name>]
[-subnet <subnet_address>] [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` is the name of the subnet you want to modify.
- `ipspace` is the name of the IPspace where the subnet resides.
- `subnet` is the new address and mask of the subnet, if applicable; for example, 192.0.2.0/24.
- `gateway` is the new gateway of the subnet, if applicable; for example, 192.0.2.1. Entering "" removes the gateway entry.
- `ip_ranges` is the new list, or range, of IP addresses that will be allocated to the subnet, if applicable. The IP addresses can be individual addresses, a range or IP addresses, or a combination in a comma-separated list. The range specified here replaces the existing IP addresses.
- `force-update-lif-associations` is required when you change the IP address range. You can set the value to `true` for this option when modifying the range of IP addresses. This command fails if any service processor or network interfaces are using the IP addresses in the specified range. Setting this value to `true` associates any manually addressed interfaces with the current subnet and allows the command to succeed.

The following command modifies the gateway IP address of subnet sub3:

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

Display subnets

You can display the list of IP addresses that are allocated to each subnet within an IPspace. The output also shows the total number of IP addresses that are available in each subnet, and the number of addresses that are currently being used.

Step

Display the list of subnets and the associated IP address ranges that are used in those subnets:

```
network subnet show
```

The following command displays the subnets and the subnet properties:

```

network subnet show

IPspace: Default
Subnet          Broadcast          Avail/
Name   Subnet      Domain    Gateway   Total   Ranges
-----  -----  -----
-----  -----
sub1   192.0.2.0/24    bcast1   192.0.2.1     5/9    192.0.2.92-
192.0.2.100
sub3   198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9

```

Delete a subnet

If you no longer need a subnet and want to deallocate the IP addresses that were assigned to the subnet, you can delete it.

About this task

You will receive an error if any service processor or network interfaces are currently using IP addresses in the specified ranges. If you want the interfaces to continue to use the IP addresses even after the subnet is deleted, you can set the `-force-update-lif-associations` option to true to remove the subnet's association with the LIFs.

Step

Delete a subnet:

```

network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]

```

The following command deletes subnet sub1 in IPspace ipspace1:

```

network subnet delete -subnet-name sub1 -ipspace ipspace1

```

Configure LIFs (cluster administrators only)

Overview

A LIF represents a network access point to a node in the cluster. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

A cluster administrator can create, view, modify, migrate, or delete LIFs. An SVM administrator can only view the LIFs associated with the SVM.

What LIFs are

A LIF (logical interface) is an IP address or WWPN with associated characteristics, such as a service policy, a home port, a home node, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network.

LIFs can be hosted on the following ports:

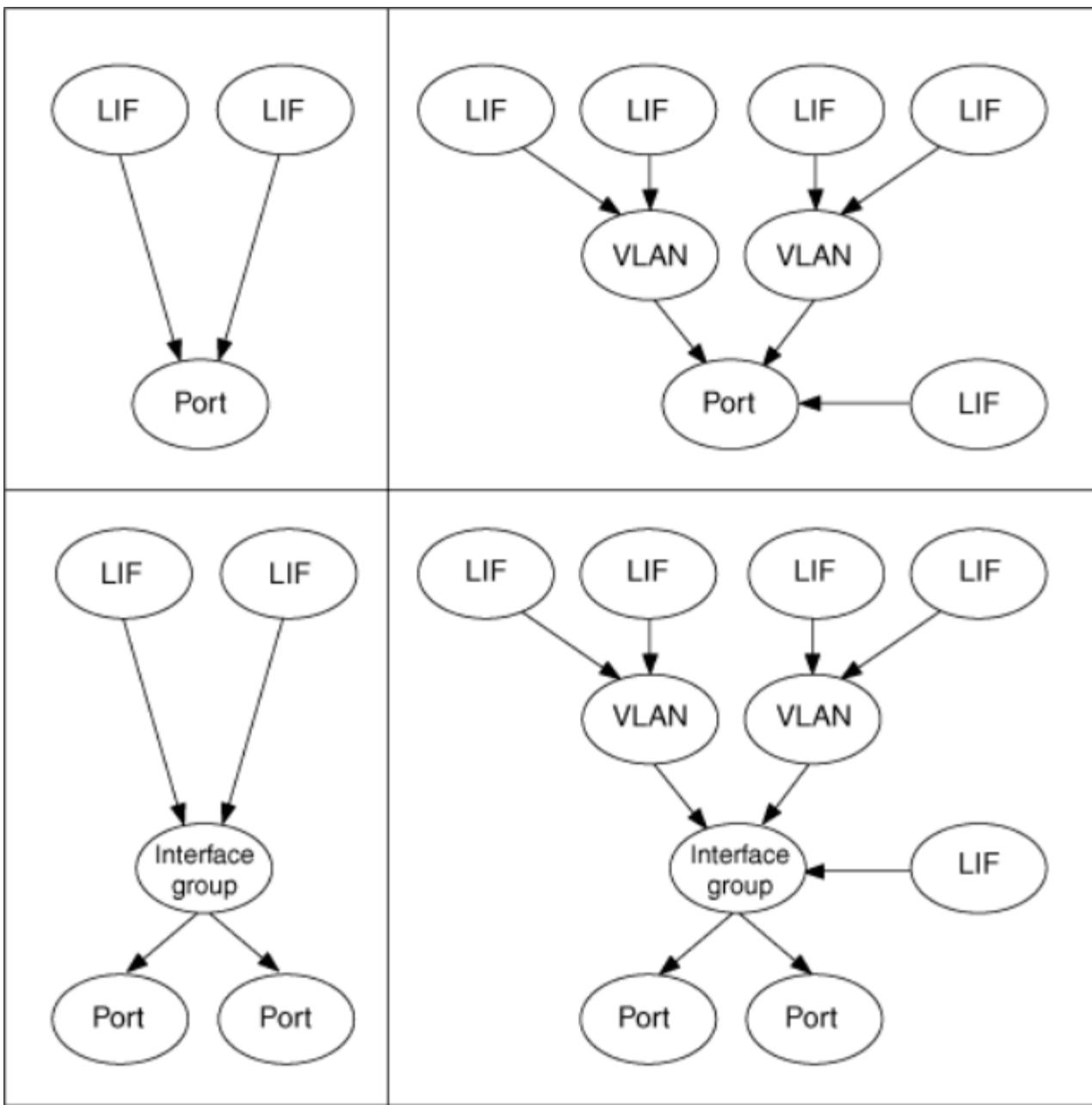
- Physical ports that are not part of interface groups
- Interface groups
- VLANs
- Physical ports or interface groups that host VLANs
- Virtual IP (VIP) ports

Starting with ONTAP 9.5, VIP LIFs are supported and are hosted on VIP ports.

While configuring SAN protocols such as FC on a LIF, it will be associated with a WWPN.

[SAN administration](#)

The following figure illustrates the port hierarchy in an ONTAP system:



LIF roles in ONTAP 9.5 and earlier

LIFs with different roles have different characteristics. A LIF role determines the kind of traffic that is supported over the interface, along with the failover rules that apply, the firewall restrictions that are in place, the security, the load balancing, and the routing behavior for each LIF. A LIF can have any one of the five roles: node management, cluster management, cluster, intercluster, and data.

Starting with ONTAP 9.6, LIF roles are deprecated. You should specify service policies for LIFs instead of a role. It is not necessary to specify a LIF role when creating a LIF with a service policy.

LIF compatibility with port types



When intercluster and management LIFs are configured in the same subnet to associate with a static route and if the route associates with an intercluster LIF, the management traffic is blocked by an external firewall and the AutoSupport and NTP connections fail. You can recover the system by running the `network interface modify -vserver vserver name -lif intercluster LIF -status-admin up|down` command to toggle the intercluster LIF. However, you should set the intercluster LIF and management LIF in different subnets to avoid this issue.

LIF role	Description
Data LIF	A LIF that is associated with a storage virtual machine (SVM) and is used for communicating with clients. You can have multiple data LIFs on a port. These interfaces can migrate or fail over throughout the cluster. You can modify a data LIF to serve as an SVM management LIF by modifying its firewall policy to mgmt. Sessions established to NIS, LDAP, Active Directory, WINS, and DNS servers use data LIFs.
Cluster LIF	A LIF that is used to carry intracluster traffic between nodes in a cluster. Cluster LIFs must always be created on 10-GbE network ports. Cluster LIFs can fail over between cluster ports on the same node, but they cannot be migrated or failed over to a remote node. When a new node joins a cluster, IP addresses are generated automatically. However, if you want to assign IP addresses manually to the cluster LIFs, you must ensure that the new IP addresses are in the same subnet range as the existing cluster LIFs.
Node management LIF	A LIF that provides a dedicated IP address for managing a particular node in a cluster. Node management LIFs are created at the time of creating or joining the cluster. These LIFs are used for system maintenance, for example, when a node becomes inaccessible from the cluster.

LIF role	Description
Cluster management LIF	<p>LIF that provides a single management interface for the entire cluster.</p> <p>A cluster management LIF can fail over to any node management or data port in the cluster. It cannot fail over to cluster or intercluster ports</p> <p>Intercluster LIF A LIF that is used for cross-cluster communication, backup, and replication. You must create an intercluster LIF on each node in the cluster before a cluster peering relationship can be established.</p> <p>These LIFs can only fail over to ports in the same node. They cannot be migrated or failed over to another node in the cluster.</p>

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Primary traffic types	NFS server, CIFS server, NIS client, Active Directory, LDAP, WINS, DNS client and server, iSCSI and FC server	Intracluster	SSH server, HTTPS server, NTP client, SNMP, AutoSupport client, DNS client, loading software updates	SSH server, HTTPS server	Cross-cluster replication

LIF security

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Require private IP subnet?	No	Yes	No	No	No
Require secure network?	No	Yes	No	No	Yes
Default firewall policy	Very restrictive	Completely open	Medium	Medium	Very restrictive
Is firewall customizable?	Yes	No	Yes	Yes	Yes

LIF failover

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
Default behavior	Only those ports in the same failover group that are on the LIF's home node and on a non-SFO partner node	Only those ports in the same failover group that are on the LIF's home node	Only those ports in the same failover group that are on the LIF's home node	Any port in the same failover group	Only those ports in the same failover group that are on the LIF's home node
Is customizable?	Yes	No	Yes	Yes	Yes

LIF routing

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
When is a default route needed?	When clients or domain controller are on different IP subnet	Never	When any of the primary traffic types require access to a different IP subnet	When administrator is connecting from another IP subnet	When other intercluster LIFs are on a different IP subnet
When is a static route to a specific IP subnet needed?	Rare	Never	Rare	Rare	When nodes of another cluster have their intercluster LIFs in different IP subnets
When is a static host route to a specific server needed?	To have one of the traffic types listed under node management LIF, go through a data LIF rather than a node management LIF. This requires a corresponding firewall change.	Never	Rare	Rare	Rare

LIF rebalancing

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
DNS: use as DNS server?	Yes	No	No	No	No

	Data LIF	Cluster LIF	Node management LIF	Cluster management LIF	Intercluster LIF
DNS: export as zone?	Yes	No	No	No	No

LIFs and service policies in ONTAP 9.6 and later

You can assign service policies (instead of LIF roles) to LIFs that determine the kind of traffic that is supported for the LIFs. Service policies define a collection of network services supported by a LIF. ONTAP provides a set of built-in service policies that can be associated with a LIF.

Service policies for system SVMs

The admin SVM and any system SVM contain service policies that can be used for LIFs in that SVM, including management and intercluster LIFs. These policies are automatically created by the system when an IPspace is created. The following table lists the built-in policies for LIFs in system SVMs:

Policy	Included services	Equivalent role	Description
default-intercluster	intercluster-core	intercluster	Used by LIFs carrying intercluster traffic. Note: Available from ONTAP 9.5 with the name net-intercluster service policy.
default-route-announce	management-bgp	-	Used by LIFs carrying BGP peer connections Note: Available from ONTAP 9.5 with the name net-route-announce service policy.
default-management	management-core, management-ems, management-ssh, management-https, management-autosupport	node-mgmt, or cluster-mgmt	Used by LIFs handling management requests. Management-ems controls which LIFs can publish EMS content.

The following table lists the services that can be used on a system SVM along with any restrictions each service imposes on a LIF's failover policy:

Service	Failover limitations	Description
intercluster-core	home-node-only	Core intercluster services
management-core	-	Core management services

Service	Failover limitations	Description
management-ssh	-	Services for SSH management access
management-https	-	Services for HTTPS management access
management-autosupport	-	Services related to posting AutoSupport payloads
management-bgp	home-port-only	Services related to BGP peer interactions

Service policies for data SVMs

All data SVMs contain service policies that can be used by LIFs in that SVM. The following table lists the built-in policies for LIFs in data SVMs:

Policy	Included services	Equivalent data protocol	Description
default-management	management-ssh, management-https	none	Used by LIFs handling management requests
default-data-blocks	data-iscsi	iscsi	Used by LIFs carrying block-oriented SAN data traffic
default-data-files	data-nfs, data-cifs, data-flexcache, data-fpolicy-client	nfs, cifs, fcache	Used by LIFs carrying file-oriented NAS data traffic.

The following table lists the services that can be used on a data SVM along with any restrictions each service imposes on a LIF's failover policy:

Policy	Included services	Equivalent data protocol	Description
management-ssh	-	-	Services for SSH management access
management-https	-	-	Services for HTTPS management access
data-core	-	data-only	Core data services (see for more details.)
data-nfs	-	data-only	Protocols related to NFS data service

Policy	Included services	Equivalent data protocol	Description
data-cifs	-	data-only	Protocols related to CIFS data service
data-flexcache	-	data-only	Protocols related to FlexCache data service
data-iscsi	home-port-only	data-only	Protocols related to iSCSI data service

You should be aware of how the service policies are assigned to the LIFs in data SVMs:

- If a data SVM is created with a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using the specified services.
- If a data SVM is created without specifying a list of data services, the built-in "default-data-files" and "default-data-blocks" service policies in that SVM are created using a default list of data services.

The default data services list includes the iSCSI, NFS, SMB, and FlexCache services.

- When a LIF is created with a list of data protocols, a service policy equivalent to the specified data protocols is assigned to the LIF.

If an equivalent service policy does not exist, a custom service policy is created.

- When a LIF is created without a service policy or list of data protocols, the default-data-files service policy is assigned to the LIF by default.

Data-core service

The data-core service allows components that previously used LIFs with the data role to work as expected on clusters that have been upgraded to manage LIFs using service policies instead of LIF roles (which are deprecated in ONTAP 9.6).

Specifying data-core as a service does not open any ports in the firewall, but the service should be included in any service policy in a data SVM. For example, the default-data-files service policy contains the following services by default:

- data-core
- data-nfs
- data-cifs
- data-flexcache

The data-core service should be included in the policy to ensure all applications using the LIF work as expected, but the other three services can be removed, if desired.

Configure LIF service policies

You can configure LIF service policies to identify a single service or a list of services that will use a LIF.

Create a service policy for LIFs

You can create a service policy for LIFs. You can assign a service policy to one or more LIFs; thereby allowing the LIF to carry traffic for a single service or a list of services.

About this task

Built-in services and service policies are available for managing data and management traffic on both data and system SVMs. Most use cases are satisfied using a built-in service policy rather than creating a custom service policy.

You can modify these built-in service policies, if required.

Steps

1. View the services that are available in the cluster:

```
network interface service show
```

Services represent the applications accessed by a LIF as well as the applications served by the cluster. Each service includes zero or more TCP and UDP ports on which the application is listening.

The following additional data and management services are available:

```
network interface service show
Service                  Protocol:Ports
-----
cluster-core             -
data-cifs                -
data-core                -
data-flexcache           -
data-iscsi               -
data-nfs                 -
intercluster-core        tcp:11104-11105
management-autosupport  -
management-bgp            tcp:179
management-core           -
management-https          tcp:443
management-ssh            tcp:22
12 entries were displayed.
```

2. Create a service policy:

```
network interface service-policy create -vserver <svm_name> -policy
<service_policy_name> -services <service_name> -allowed-addresses
<IP_address/mask,...>
```

- "service_name" specifies a list of services that should be included in the policy.

- "IP_address/mask" specifies the list of subnet masks for addresses that are allowed to access the services in the service policy. By default, all specified services are added with a default allowed address list of 0.0.0.0/0, which allows traffic from all subnets. When a non-default allowed address list is provided, LIFs using the policy are configured to block all requests with a source address that does not match any of the specified masks.

The following example shows how to create a data service policy, `svm1_data_policy`, for an SVM that includes NFS and SMB services:

```
network interface service-policy create -vserver svm1 -policy
svm1_data_policy - services data-nfs,data-cifs,data-core -allowed-
addresses 10.1.0.0/16
```

The following example shows how to create an intercluster service policy:

```
network interface service-policy create -vserver cluster1 -policy
intercluster1 - services intercluster-core -allowed-addresses
10.1.0.0/16
```

3. Verify that the service policy is created.

```
network interface service-policy show
```

The following output shows the service policies that are available:

```

network interface service-policy show
Vserver   Policy                               Service: Allowed Addresses
----- -----
----- 

cluster1
    default-intercluster          intercluster-core: 0.0.0.0/0
                                    management-https: 0.0.0.0/0

    default-management           management-core: 0.0.0.0/0
                                    management-autosupport: 0.0.0.0/0
                                    management-ssh: 0.0.0.0/0
                                    management-https: 0.0.0.0/0

    default-route-announce      management-bgp: 0.0.0.0/0

Cluster
    default-cluster             cluster-core: 0.0.0.0/0

vs0
    default-data-blocks         data-core: 0.0.0.0/0
                                    data-iscsi: 0.0.0.0/0

    default-data-files          data-core: 0.0.0.0/0
                                    data-nfs: 0.0.0.0/0
                                    data-cifs: 0.0.0.0/0
                                    data-flexcache: 0.0.0.0/0

    default-management          data-core: 0.0.0.0/0
                                    management-ssh: 0.0.0.0/0
                                    management-https: 0.0.0.0/0

7 entries were displayed.

```

After you finish

Assign the service policy to a LIF either at the time of creation or by modifying an existing LIF.

Assign a service policy to a LIF

You can assign a service policy to a LIF either at the time of creating the LIF or by modifying the LIF. A service policy defines the list of services that can be used with the LIF.

About this task

You can assign service policies for LIFs in the admin and data SVMs.

Step

Depending on when you want to assign the service policy to a LIF, perform one of the following actions:

If you are...	Assign the service policy by entering the following command...
Creating a LIF	network interface create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> {(-address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
Modifying a LIF	network interface modify -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

When you specify a service policy for a LIF, you need not specify the data protocol and role for the LIF. Creating LIFs by specifying the role and data protocols is also supported.



A service policy can only be used by LIFs in the same SVM that you specified when creating the service policy.

Examples

The following example shows how to modify the service policy of a LIF to use the default- management service policy:

```
network interface modify -vserver cluster1 -lif lif1 -service-policy
default-management
```

Commands for managing LIF service policies

Use the `network interface service-policy` commands to manage LIF service policies.

If you want to...	Use this command...
Create a service policy	<code>network interface service-policy create</code>
Add an additional service entry to an existing service policy	<code>network interface service-policy add-service</code>
Clone an existing service policy	<code>network interface service-policy clone</code>
Modify a service entry in an existing service policy	<code>network interface service-policy modify-service</code>
Remove a service entry from an existing service policy	<code>network interface service-policy remove-service</code>
Rename an existing service policy	<code>network interface service-policy rename</code>
Delete an existing service policy	<code>network interface service-policy delete</code>

If you want to...	Use this command...
Restore a built-in service-policy to its original state	<code>network interface service-policy restore-defaults</code>
Display existing service policies	<code>network interface service-policy show</code>

Create a LIF

A LIF is an IP address associated with a physical or logical port. If there is a component failure, a LIF can fail over to or be migrated to a different physical port, thereby continuing to communicate with the network.

Before you begin

- The underlying physical or logical network port must have been configured to the administrative up status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

- The mechanism for specifying the type of traffic handled by a LIF has changed. For ONTAP 9.5 and earlier, LIFs used roles to specify the type of traffic it would handle. Starting in ONTAP 9.6, LIFs use service policies to specify the type of traffic it would handle.

About this task

- You cannot assign NAS and SAN protocols to the same LIF.

The supported protocols are SMB, NFS, FlexCache, iSCSI, and FC; iSCSI and FC cannot be combined with other protocols. However, NAS and Ethernet-based SAN protocols can be present on the same physical port.

- You can create both IPv4 and IPv6 LIFs on the same network port.
- All the name mapping and host-name resolution services used by an SVM, such as DNS, NIS, LDAP, and Active Directory, must be reachable from at least one LIF handling data traffic of the SVM.
- A LIF handling intracluster traffic between nodes should not be on the same subnet as a LIF handling management traffic or a LIF handling data traffic.
- Creating a LIF that does not have a valid failover target results in a warning message.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).
- Starting with ONTAP 9.7, if other LIFs already exist for the SVM in the same subnet, you do not need to specify the home port of the LIF. ONTAP automatically chooses a random port on the specified home node in the same broadcast domain as the other LIFs already configured in the same subnet.

Beginning in ONTAP 9.4, FC-NVMe is supported. If you are creating an FC-NVMe LIF you should be aware of the following:

- The NVMe protocol must be supported by the FC adapter on which the LIF is created.
- FC-NVMe can be the only data protocol on data LIFs.
- One LIF handling management traffic must be configured for every storage virtual machine (SVM) supporting SAN.
- NVMe LIFs and namespaces must be hosted on the same node.
- Only one NVMe LIF handling data traffic can be configured per SVM.

Steps

1. Create a LIF:

```
network interface create -vserver vserver_name -lif lif_name -service
-priority priority -home-node node_name -home-port port_name {-
-address IP_address - netmask IP_address | -subnet-name subnet_name}
-firewall- policy policy -auto-revert {true|false}
```

- `-home-node` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

- `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.
- When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create` man page contains information about creating a static route within an SVM.
- `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `true` depending on network management policies in your environment.
- `-service-policy` Starting with ONTAP 9.5, you can assign a service policy for the LIF with the `-service-policy` option.

When a service policy is specified for a LIF, the policy is used to construct a default role, failover policy, and data protocol list for the LIF. In ONTAP 9.5, service policies are supported only for intercluster and BGP peer services. In ONTAP 9.6, you can create service policies for several data and management services.

- `-data-protocol` allows you to create a LIF that supports the Fibre Channel Protocol (FCP) or NVMe/FC protocols. This option is not required when creating an IP LIF.

2. Optional: If you want to assign an IPv6 address in the `-address` option:

- a. Use the `network ndp prefix show` command to view the list of RA prefixes learned on various interfaces.

The `network ndp prefix show` command is available at the advanced privilege level.

- b. Use the format `prefix::id` to construct the IPv6 address manually.

`prefix` is the prefix learned on various interfaces.

For deriving the `id`, choose a random 64-bit hexadecimal number.

3. Verify that the LIF was created successfully by using the `network interface show` command.
4. Verify that the configured IP address is reachable:

To verify an...	Use...
IPv4 address	<code>network ping</code>
IPv6 address	<code>network ping6</code>

Examples

The following command creates a LIF and specifies the IP address and network mask values using the `-address` and `-netmask` parameters:

```
network interface create -vserver vs1.example.com -lif datalif1 -service
-priority default-data-files -home-node node-4 -home-port e1c -address
192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

The following command creates a LIF and assigns IP address and network mask values from the specified subnet (named `client1_sub`):

```
network interface create -vserver vs3.example.com -lif datalif3 -service
-priority default-data-files -home-node node-3 -home-port e1c -subnet-name
client1_sub - auto-revert true
```

The following command creates an NVMe/FC LIF and specifies the `nvme-fc` data protocol:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

Modify a LIF

You can modify a LIF by changing the attributes, such as home node or current node, administrative status, IP address, netmask, failover policy, firewall policy, and service policy. You can also change the address family of a LIF from IPv4 to IPv6.

About this task

- When modifying a LIF's administrative status to down, any outstanding NFSv4 locks are held until the LIF's administrative status is returned to up.

To avoid lock conflicts that can occur when other LIFs attempt to access the locked files, you must move the NFSv4 clients to a different LIF before setting the administrative status to down.

- You cannot modify the data protocols used by an FC LIF. However, you can modify the services assigned to a service policy or change the service policy assigned to an IP LIF.

To modify the data protocols used by a FC LIF, you must delete and re-create the LIF. To make service policy changes to an IP LIF, there is a brief outage while the updates occur.

- You cannot modify either the home node or the current node of a node-scoped management LIF.
- When using a subnet to change the IP address and network mask value for a LIF, an IP address is allocated from the specified subnet; if the LIF's previous IP address is from a different subnet, the IP address is returned to that subnet.
- To modify the address family of a LIF from IPv4 to IPv6, you must use the colon notation for the IPv6 address and add a new value for the `-netmask-length` parameter.
- You cannot modify the auto-configured link-local IPv6 addresses.
- Modification of a LIF that results in the LIF having no valid failover target results in a warning message.

If a LIF that does not have a valid failover target attempts to fail over, an outage might occur.

- Starting with ONTAP 9.5, you can modify the service policy associated with a LIF.

In ONTAP 9.5, service policies are supported only for intercluster and BGP peer services. In ONTAP 9.6, you can create service policies for several data and management services.

Steps

- Modify a LIF's attributes by using the "network interface modify" command.

The following example shows how to modify the IP address and network mask of LIF `datalif2` using an IP address and the network mask value from subnet `client1_sub`:

```
network interface modify -vserver vs1 -lif datalif2 -subnet-name
client1_sub
```

The following example shows how to modify the service policy of a LIF.

```
network interface modify -vserver siteA -lif node1_inter1 -service
-policy example
```

- Verify that the IP addresses are reachable.

If you are using...	Then use...
IPv4 addresses	<code>network ping</code>

If you are using...	Then use...
IPv6 addresses	<code>network ping6</code>

Migrate a LIF

You might have to migrate a LIF to a different port on the same node or a different node within the cluster, if the port is either faulty or requires maintenance. Migrating a LIF is similar to LIF failover, but LIF migration is a manual operation, while LIF failover is the automatic migration of a LIF in response to a link failure on the LIF's current network port.

Before you begin

- A failover group must have been configured for the LIFs.
- The destination node and ports must be operational and must be able to access the same network as the source port.

About this task

- You must migrate LIFs hosted on the ports belonging to a NIC to other ports in the cluster, before removing the NIC from the node.
- You must execute the command for migrating a cluster LIF from the node where the cluster LIF is hosted.
- A node-scoped LIF, such as a node-scoped management LIF, cluster LIF, intercluster LIF, cannot be migrated to a remote node.
- When an NFSv4 LIF is migrated between nodes, a delay of up to 45 seconds results before the LIF is available on a new port.

To work around this problem, use NFSv4.1 where no delay is encountered.

- You cannot migrate iSCSI LIFs from one node to another node.

To work around this restriction, you must create an iSCSI LIF on the destination node. For information about guidelines for creating an iSCSI LIF, see [SAN administration](#).

- VMware VAAI copy offload operations fail when you migrate the source or the destination LIF. For more information about VMware VAAI, see [NFS reference](#) or [SAN administration](#).

Step

Depending on whether you want to migrate a specific LIF or all the LIFs, perform the appropriate action:

If you want to migrate...	Enter the following command...
A specific LIF	<code>network interface migrate</code>
All the data and cluster- management LIFs on a node	<code>network interface migrate-all</code>
All of the LIFs off of a port	<code>network interface migrate-all -node <node> -port <port></code>

The following example shows how to migrate a LIF named `datalif1` on the SVM `vs0` to the port `e0d` on node0b:

```
network interface migrate -vserver vs0 -lif data1if1 -dest-node node0b  
-dest-port e0d
```

The following example shows how to migrate all the data and cluster-management LIFs from the current (local) node:

```
network interface migrate-all -node local
```

Revert a LIF to its home port

You can revert a LIF to its home port after it fails over or is migrated to a different port either manually or automatically. If the home port of a particular LIF is unavailable, the LIF remains at its current port and is not reverted.

About this task

- If you administratively bring the home port of a LIF to the up state before setting the automatic revert option, the LIF is not returned to the home port.
- The node management LIF does not automatically revert unless the value of the "auto-revert" option is set to true.
- You must ensure that the "auto-revert" option is enabled for the cluster LIFs to revert to their home ports.

Step

Revert a LIF to its home port manually or automatically:

If you want to revert a LIF to its home port...	Then enter the following command...
Manually	network interface revert -vserver vserver_name -lif lif_name
Automatically	network interface modify -vserver vserver_name -lif lif_name -auto-revert true

ONTAP 9.8 and later: Recover from an incorrectly configured cluster LIF

A cluster cannot be created when the cluster network is cabled to a switch but not all of the ports configured in the Cluster IPspace can reach the other ports configured in the Cluster IPspace.

About this task

In a switched cluster, if a cluster network interface (LIF) is configured on the wrong port, or if a cluster port is wired into the wrong network, the `cluster create` command can fail with the following error:

Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.

The results of the `network port show` command might show that several ports are added to the Cluster

IPspace because they are connected to a port that is configured with a cluster LIF. However, the results of the `network port reachability show -detail` command reveal which ports do not have connectivity to one another.

To recover from a cluster LIF configured on a port that is not reachable to the other ports configured with cluster LIFs, perform the following steps:

Steps

1. Reset the home port of the cluster LIF to the correct port:

```
net port modify -home-port
```

2. Remove the ports that do not have cluster LIFs configured on them from the cluster broadcast domain:

```
net port broadcast-domain remove-ports
```

3. Create the cluster:

```
cluster create
```

Result

When you complete the cluster creation, the system detects the correct configuration and places the ports into the correct broadcast domains.

Delete a LIF

You can delete a network interface (LIF) that is no longer required.

Before you begin

LIFs to be deleted must not be in use.

Steps

1. Mark the LIFs you want to delete as administratively down using the following command:

```
-status-admin down
```

2. Use the `network interface delete` command to delete one or all LIFs:

If you want to delete...	Enter the command ...
A specific LIF	<code>network interface delete -lif lif_name</code>
All LIFs	<code>network interface delete -lif</code>

The following command deletes the LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Use the `network interface show` command to confirm that the LIF is deleted.

Configure virtual IP (VIP) LIFs

Some next-generation data centers use Network-Layer-3 mechanisms that require LIFs to be failed over across subnets. Starting with ONTAP 9.5, VIP data LIFs and the associated routing protocol, border gateway protocol (BGP), are supported, which enable ONTAP to participate in these next-generation networks.

About this task

A VIP data LIF is a LIF that is not part of any subnet and is reachable from all ports that host a BGP LIF in the same IPspace. A VIP data LIF eliminates the dependency of a host on individual network interfaces. Because multiple physical adapters carry the data traffic, the entire load is not concentrated on a single adapter and the associated subnet. The existence of a VIP data LIF is advertised to peer routers through the routing protocol, Border Gateway Protocol (BGP).

VIP data LIFs provide the following advantages:

- LIF portability beyond a broadcast domain or subnet: VIP data LIFs can fail over to any subnet in the network by announcing the current location of each VIP data LIF to routers through BGP.
- Aggregate throughput: VIP data LIFs can support aggregate throughput that exceeds the bandwidth of any individual port because the VIP LIFs can send or receive data from multiple subnets or ports simultaneously.

Set up border gateway protocol (BGP)

Before creating VIP LIFs, you must set up BGP, which is the routing protocol used for announcing the existence of a VIP LIF to peer routers.

Starting with ONTAP 9.9.1, VIP BGP provides default route automation using BGP peer grouping to simplify configuration.

ONTAP has a simple way to learn default routes using the BGP peers as next-hop routers when the BGP peer is on the same subnet. To use the feature, set the `-use-peer-as-next-hop` attribute to `true`. By default, this attribute is `false`.

If you have static routes configured, those are still preferred over these automated default routes.

Before you begin

The peer router must be configured to accept a BGP connection from the BGP LIF for the configured autonomous system number (ASN).



ONTAP does not process any incoming route announcements from the router; therefore, you should configure the peer router to not send any route updates to the cluster.

About this task

Setting up BGP involves optionally creating a BGP configuration, creating a BGP LIF, and creating a BGP peer group. ONTAP automatically creates a default BGP configuration with default values when the first BGP peer

group is created on a given node. A BGP LIF is used to establish BGP TCP sessions with peer routers. For a peer router, a BGP LIF is the next hop to reach a VIP LIF. Failover is disabled for the BGP LIF. A BGP peer group advertises the VIP routes for all the SVMs in the peer group's IPspace.

Starting with ONTAP 9.8, these fields have been added to the `network bgp peer-group` command:

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

These BGP attributes allows you to configure the AS Path and community attributes for the BGP peer group.

Starting with ONTAP 9.9.1, these fields have been added:

- `-asn` or `-peer-asn` (4-byte value)
The attribute itself is not new, but it now uses a 4-byte integer.
- `-med`
- `-use-peer-as-next-hop`

You can make advanced route selections with Multi-Exit Discriminator (MED) support for path prioritization. MED is an optional attribute in the BGP update message that tells routers to select the best route for the traffic. The MED is an unsigned 32-bit integer (0 - 4294967295); lower values are preferred.



While ONTAP supports the above BGP attributes, routers need not honor them. NetApp highly recommends you confirm which attributes are supported by your router and configure BGP peer-groups accordingly. For details, refer to the BGP documentation provided by your router.

Steps

1. Log in to the advanced privilege level:

```
set -privilege advanced
```

2. Optional: Create a BGP configuration or modify the default BGP configuration of the cluster by performing one of the following actions:

- a. Create a BGP configuration:

```
network bgp config create -node {node_name | local} -asn asn_integer
-holdtime
hold_time -routerid local_router_IP_address
```

Sample with a 2-byte ASN:

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

Sample with a 4-byte ASN:

```
network bgp config create -node node1 -asn 85502 -holdtime 180  
-routerid 1.1.1.1
```

b. Modify the default BGP configuration:

```
network bgp defaults modify -asn asn_integer -holdtime hold_time  
network bgp defaults modify -asn 65502
```

- **asn_integer** specifies the ASN. Starting in ONTAP 9.8, ASN for BGP supports a 2-byte non-negative integer. This is a 16-bit number (0 - 64511 available values). Starting in ONTAP 9.9.1, ASN for BGP supports a 4-byte non-negative integer (65536 - 4294967295). The default ASN is 65501. ASN 23456 is reserved for ONTAP session establishment with peers that do not announce 4-byte ASN capability.
- **hold_time** specifies the hold time in seconds. The default value is 180s.

3. Create a BGP LIF for the system SVM:

```
network interface create -vserver system_svm -lif lif_name -service  
-policy default-route-announce -home-node home_node -home-port home_port  
-address ip_address -netmask netmask
```

You can use the **default-route-announce** service policy for the BGP LIF.

```
network interface create -vserver cluster1 -lif bgp1 -service-policy  
default-route-announce -home-node cluster1-01 -home-port e0c -address  
10.10.10.100 -netmask 255.255.255.0
```

4. Create a BGP peer group that is used to establish BGP sessions with the remote peer routers and configure the VIP route information that is advertised to the peer routers:

Sample 1: Create a peer group without an auto default route

In this case, the admin has to create a static route to the BGP peer.

```
network bgp peer-group create -peer-group group_name -ipspace  
ipspace_name -bgp-lif bgp_lif -peer-address peer-router_ip_address -peer  
-asn 65502 -route-preference integer  
-asn-prepend-type <ASN_prepend_type> -asn-prepend-count integer -med  
integer -community BGP community list <0-65535>:<0-65535>
```

```
network bgp peer-group create -peer-group group1 -ipspc Default -bgp  
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65502 -route-preference 100  
-asn-prepend-type local ASN -asn-prepend-count 2 -med 100 -community  
9000:900,8000:800
```

Sample 2: Create a peer group with an auto default route

```
network bgp peer-group create -peer-group group_name -ipspc  
ipspc_name -bgp-lif bgp_lif -peer-address peer-router_ip_address -peer  
-asn 65502 -use-peer-as-next-hop true -route-preference integer -asn  
-prepend-type <ASN_prepending_type> -asn-prepend-count integer -med integer  
-community BGP community list <0-65535>:<0-65535>
```

```
network bgp peer-group create -peer-group group1 -ipspc Default -bgp  
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65502 -use-peer-as-next-hop  
true -route-preference 100 -asn-prepend-type local ASN -asn-prepend  
-count 2 -med 100 -community 9000:900,8000:800
```

Create a virtual IP (VIP) data LIF

The existence of a VIP data LIF is advertised to peer routers through the routing protocol, Border Gateway Protocol (BGP).

Before you begin

- The BGP peer group must be set up and the BGP session for the SVM on which the LIF is to be created must be active.
- A static route to the BGP router or any other router in the BGP LIF's subnet must be created for any outgoing VIP traffic for the SVM.
- You should turn on multipath routing so that the outgoing VIP traffic can utilize all the available routes.

If multipath routing is not enabled, all the outgoing VIP traffic goes from a single interface.

Steps

1. Create a VIP data LIF:

```
network interface create -vserver svm_name -lif lif_name -role data  
-data-protocol  
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node home_node -address  
ip_address -is-vip true
```

A VIP port is automatically selected if you do not specify the home port with the [network interface create](#) command.

By default, the VIP data LIF belongs to the system-created broadcast domain named 'Vip', for each IPspace. You cannot modify the VIP broadcast domain.

A VIP data LIF is reachable simultaneously on all ports hosting a BGP LIF of an IPspace. If there is no active BGP session for the VIP's SVM on the local node, the VIP data LIF fails over to the next VIP port on the node that has a BGP session established for that SVM.

2. Verify that the BGP session is in the up status for the SVM of the VIP data LIF:

```
network bgp vserver-status show

Node          Vserver    bgp status
-----  -----
node1        vs1         up
```

If the BGP status is `down` for the SVM on a node, the VIP data LIF fails over to a different node where the BGP status is up for the SVM. If BGP status is `down` on all the nodes, the VIP data LIF cannot be hosted anywhere, and has LIF status as down.

Commands for managing the BGP

Starting with ONTAP 9.5, you use the `network bgp` commands to manage the BGP sessions in ONTAP.

Manage BGP configuration

If you want to...	Use this command...
Create a BGP configuration	<code>network bgp config create</code>
Modify BGP configuration	<code>network bgp config modify</code>
Delete BGP configuration	<code>network bgp config delete</code>
Display BGP configuration	<code>network bgp config show</code>
Displays the BGP status for the SVM of the VIP LIF	<code>network bgp vserver-status show</code>

Manage BGP default values

If you want to...	Use this command...
Modify BGP default values	<code>network bgp defaults modify</code>
Display BGP default values	<code>network bgp defaults show</code>

Manage BGP peer groups

If you want to...	Use this command...
Create a BGP peer group	<code>network bgp peer-group create</code>
Modify a BGP peer group	<code>network bgp peer-group modify</code>
Delete a BGP peer group	<code>network bgp peer-group delete</code>

If you want to...	Use this command...
Display BGP peer groups information	network bgp peer-group show
Rename a BGP peer group	network bgp peer-group rename

Related information: [ONTAP 9 commands](#)

Configure host-name resolution

Overview

ONTAP must be able to translate host names to numerical IP addresses in order to provide access to clients and to access services. You must configure storage virtual machines (SVMs) to use local or external name services to resolve host information. ONTAP supports configuring an external DNS server or configuring the local hosts file for host name resolution.

When using an external DNS server, you can configure Dynamic DNS (DDNS), which automatically sends new or changed DNS information from your storage system to the DNS server. Without dynamic DNS updates, you must manually add DNS information (DNS name and IP address) to the identified DNS servers when a new system is brought online or when existing DNS information changes. This process is slow and error-prone. During disaster recovery, manual configuration can result in a long downtime.

Configure DNS for host-name resolution

You use DNS to access either local or remote sources for host information. You must configure DNS to access one or both of these sources.

ONTAP must be able to look up host information to provide proper access to clients. You must configure name services to enable ONTAP to access local or external DNS services to obtain the host information.

ONTAP stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems.

Configure an SVM and data LIFs for host-name resolution using an external DNS server

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

Before you begin

A site-wide DNS server must be available for host name lookups.

You should configure more than one DNS server to avoid a single-point-of-failure. The `vserver services name-service dns create` command issues a warning if you enter only one DNS server name.

About this task

The Network Management Guide contains information about configuring dynamic DNS on the SVM.

Steps

1. Enable DNS on the SVM:

```
vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled
```

The following command enables external DNS server servers on the SVM vs1:

```
vserver services name-service dns create -vserver <vs1.example.com> -domains <example.com> -name-servers <192.0.2.201,192.0.2.202> -state <enabled>
```



The vserver services name-service dns create command performs an automatic configuration validation and reports an error message if ONTAP cannot contact the name server.

2. Enable DNS on LIFs owned by the SVM:

If you are	Use this command:
Modifying an existing LIF zone-name	network interface modify -lif lifname -dns-zone
Creating a new LIF zone-name	network interface create -lif lifname -dns-zone

```
vserver services name-service dns create -vserver <vs1> -domains <example.com> -name-servers <192.0.2.201, 192.0.2.202> -state <enabled>
network interface modify -lif <datalif1> -dns-zone <zonename.whatever.com>
```

3. Validate the status of the name servers by using the `vserver services name-service dns check` command.

```
vserver services name-service dns check -vserver vs1.example.com
VserverName      Server      Status      Status Details
-----          -----
vs1.example.com  10.0.0.50  up          Response time (msec): 2
vs1.example.com  10.0.0.51  up          Response time (msec): 2
```

Configure the Name Service Switch Table for Host-Name Resolution

You must configure the name service switch table correctly to enable ONTAP to consult local or external name service to retrieve host information.

Before you begin

You must have decided which name service to use for host mapping in your environment.

Steps

1. Add the necessary entries to the name service switch table:

```
vserver services name-service <ns-switch> create -vserver <vserver_name>  
-database <database_name> -source <source_names>
```

2. Verify that the name service switch table contains the expected entries in the desired order:

```
vserver services name-service <ns-switch> show -vserver <vserver_name>
```

Example

The following example creates an entry in the name service switch table for SVM vs1 to first use the local hosts file and then an external DNS server to resolve host names:

```
vserver services name-service ns-switch create -vserver vs1 -database  
hosts -sources files dns
```

Manage the hosts table (cluster administrators only)

A cluster administrator can add, modify, delete, and view the host name entries in the hosts table of the admin storage virtual machine (SVM). An SVM administrator can configure the host name entries only for the assigned SVM.

Commands for managing local host-name entries

You can use the `vserver services name-service dns hosts` command to create, modify, or delete DNS host table entries.

When you are creating or modifying the DNS host-name entries, you can specify multiple alias addresses separated by commas.

If you want to...	Use this command...
Create a DNS host-name entry	<code>vserver services name-service dns hosts create</code>
Modify a DNS host-name entry	<code>vserver services name-service dns hosts modify</code>
Delete a DNS host-name entry	<code>vserver services name-service dns hosts delete</code>

For more information, see the [ONTAP 9 commands](#) for the `vserver services name-service dns hosts` commands.

Balance network loads to optimize user traffic (cluster administrators only)

Overview

You can configure your cluster to serve client requests from appropriately loaded LIFs. This results in a more balanced utilization of LIFs and ports, which in turn allows for better performance of the cluster.

What DNS load balancing is

DNS load balancing helps in selecting an appropriately loaded data LIF and balancing user network traffic across all available ports (physical, interface groups, and VLANs).

With DNS load balancing, LIFs are associated with the load balancing zone of an SVM. A site-wide DNS server is configured to forward all DNS requests and return the least-loaded LIF based on the network traffic and the availability of the port resources (CPU usage, throughput, open connections, and so on). DNS load balancing provides the following benefits:

- New client connections balanced across available resources.
- No manual intervention required for deciding which LIFs to use when mounting a particular SVM.
- DNS load balancing supports NFSv3, NFSv4, NFSv4.1, CIFS, SMB 2.0, SMB 2.1, and SMB 3.0.

How DNS load balancing works

Clients mount an SVM by specifying an IP address (associated with a LIF) or a host name (associated with multiple IP addresses). By default, LIFs are selected by the site-wide DNS server in a round-robin manner, which balances the workload across all LIFs.

Round-robin load balancing can result in overloading some LIFs, so you have the option of using a DNS load balancing zone that handles the host-name resolution in an SVM. Using a DNS load balancing zone, ensures better balance of the new client connections across available resources, leading to improved performance of the cluster.

A DNS load balancing zone is a DNS server inside the cluster that dynamically evaluates the load on all LIFs and returns an appropriately loaded LIF. In a load balancing zone, DNS assigns a weight (metric), based on the load, to each LIF.

Every LIF is assigned a weight based on its port load and CPU utilization of its home node. LIFs that are on less-loaded ports have a higher probability of being returned in a DNS query. Weights can also be manually assigned.

Create a DNS load balancing zone

You can create a DNS load balancing zone to facilitate the dynamic selection of a LIF based on the load, that is, the number of clients mounted on a LIF. You can create a load balancing zone while creating a data LIF.

Before you begin

The DNS forwarder on the site-wide DNS server must be configured to forward all requests for the load balancing zone to the configured LIFs.

The Knowledgebase article [How to set up DNS load balancing in Cluster-Mode](#) on the NetApp Support Site contains more information about configuring DNS load balancing using conditional forwarding.

About this task

- Any data LIF can respond to DNS queries for a DNS load balancing zone name.
- A DNS load balancing zone must have a unique name in the cluster, and the zone name must meet the following requirements:
 - It should not exceed 256 characters.
 - It should include at least one period.
 - The first and the last character should not be a period or any other special character.
 - It cannot include any spaces between characters.
 - Each label in the DNS name should not exceed 63 characters.

A label is the text appearing before or after the period. For example, the DNS zone named storage.company.com has three labels.

Step

Use the `network interface create` command with the `dns-zone` option to create a DNS load balancing zone.

If the load balancing zone already exists, the LIF is added to it. For more information about the command, see [ONTAP 9 commands](#).

The following example demonstrates how to create a DNS load balancing zone named storage.company.com while creating the LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1  
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
```

Add or remove a LIF from a load balancing zone

You can add or remove a LIF from the DNS load balancing zone of a storage virtual machine (SVM). You can also remove all the LIFs simultaneously from a load balancing zone.

Before you begin

- All the LIFs in a load balancing zone should belong to the same SVM.
- A LIF can be a part of only one DNS load balancing zone.
- Failover groups for each subnet must have been set up, if the LIFs belong to different subnets.

About this task

A LIF that is in the administrative down status is temporarily removed from the DNS load balancing zone. When the LIF returns to the administrative up status, the LIF is automatically added to the DNS load balancing zone.

Step

Add a LIF to or remove a LIF from a load balancing zone:

If you want to...	Enter...
Add a LIF	<pre>network interface modify -vserver vserver_name -lif lif_name-dns-zone zone_name</pre> <p>Example:</p> <pre>network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com</pre>
Remove a single LIF	<pre>network interface modify -vserver vserver_name -lif lif_name-dns-zone none</pre> <p>Example:</p> <pre>network interface modify -vserver vs1 -lif data1 -dns -zone none</pre>
Remove all LIFs	<pre>network interface modify -vserver vserver_name -lif * -dns-zone none</pre> <p>Example:</p> <pre>network interface modify -vserver vs0 -lif * -dns-zone none</pre> <p>You can remove an SVM from a load balancing zone by removing all the LIFs in the SVM from that zone.</p>

Secure your network

Configure network security using federal information processing standards (FIPS)

ONTAP is compliant in the Federal Information Processing Standards (FIPS) 140-2 for all SSL connections. You can turn on and off SSL FIPS mode, set SSL protocols globally, and turn off any weak ciphers such as RC4 within ONTAP.

By default, SSL on ONTAP is set with FIPS compliance disabled and SSL protocol enabled with the following:

- TLSv1.2
- TLSv1.1
- TLSv1

When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

Enable FIPS

It is recommended that all secure users adjust their security configuration immediately after system installation or upgrade. When SSL FIPS mode is enabled, SSL communication from ONTAP to external client or server components outside of ONTAP will use FIPS compliant crypto for SSL.

About this task

The following settings are recommended to enable FIPS:

- `FIPS: on`
- `SSL protocol = {TLSv1.2}`

- `SSL ciphers = {ALL:!LOW:!aNULL:!EXP:!eNULL:!RC4}`

Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Enable FIPS:

```
security config modify -interface SSL -is-fips-enabled true
```

3. When prompted to continue, enter `y`

4. One by one, manually reboot each node in the cluster.

Example

```
security config modify -interface SSL -is-fips-enabled true
```

Warning: This command will enable FIPS compliance and can potentially cause some non-compliant components to fail. MetroCluster and Vserver DR require FIPS to be enabled on both sites in order to be compatible.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

Disable FIPS

If you are still running an older system configuration and want to configure ONTAP with backward compatibility, you can turn on SSLv3 only when FIPS is disabled.

About this task

The following settings are recommended to disable FIPS:

- `FIPS = false`
- `SSL protocol = {SSLv3}`
- `SSL ciphers = {ALL:!LOW:!aNULL:!EXP:!eNULL}`

Steps

1. Change to advanced privilege level:

```
set -privilege advanced
```

2. Disable FIPS by typing:

```
security config modify -interface SSL -supported-protocols SSLv3
```

3. When prompted to continue, enter **y**.

4. Manually reboot each node in the cluster.

Example

```
security config modify -interface SSL -supported-protocols SSLv3
```

Warning: Enabling the SSLv3 protocol may reduce the security of the interface, and is not recommended.

Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster. This is necessary to prevent components from failing due to an inconsistent security configuration state in the cluster. To avoid a service outage, reboot one node at a time and wait for it to completely initialize before rebooting the next node. Run "security config status show" command to monitor the reboot status.

Do you want to continue? {y|n}: y

View FIPS compliance status

You can see whether the entire cluster is running the current security configuration settings.

Steps

1. One by one, reboot each node in the cluster.

Do not reboot all cluster nodes simultaneously. A reboot is required to make sure that all applications in the cluster are running the new security configuration, and for all changes to FIPS on/off mode, Protocols, and Ciphers.

2. View the current compliance status:

```
security config show
```

Example

```
security config show

      Cluster          Cluster
Security
Interface FIPS Mode  Supported Protocols    Supported Ciphers Config
Ready

-----
-----
SSL       false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL: yes
                           !EXP:!eNULL
```

Configure IP security (IPsec) over wire encryption

Starting with ONTAP 9.8, ONTAP uses the IPsec protocol in transport mode to ensure data is continuously secure and encrypted, even while in transit. IPsec offers data encryption for all IP traffic including the NFS, iSCSI, and SMB/CIFS protocols. IPsec provides the only encryption in flight option for iSCSI traffic.

While IPsec capability is enabled on the cluster, the network requires a Security Policy Database (SPD) entry and a preshared secret on the client before traffic can flow.

After IPsec is configured, network traffic between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.

For NetApp SnapMirror and cluster peering traffic encryption, cluster peering encryption (CPE) is still recommended over IPsec for secure in-transit over the wire. This is because CPE has better performance than IPsec. You do not require a license for IPsec and there are no import or export restrictions.

Enable IPsec on the cluster

You can enable Internet Protocol security (IPsec) on the cluster to ensure data is continuously secure and encrypted, even while in transit.

Steps

1. Discover if IPsec is enabled already:

```
security ipsec config show
```

If the result includes `IPsec Enabled: false`, proceed to the next step.

2. Enable IPsec:

```
security ipsec config modify -is-enabled true
```

3. Run the discovery command again:

```
security ipsec config show
```

The result now includes `IPsec Enabled: true`.

Define the security policy database (SPD)

IPsec requires an SPD entry before allowing traffic to flow on the network.

Step

1. Use the `security ipsec policy create` command to:
 - a. Select the ONTAP IP address or subnet of IP addresses to participate in the IPsec transport.
 - b. Select the client IP addresses that will connect to the ONTAP IP addresses.

 The client must support Internet Key Exchange version 2 (IKEv2) with a pre-shared key (PSK).

c. Optional. Select the upper layer protocols (UDP, TCP, ICMP, etc.), the local port numbers, and the remote port numbers to protect. The corresponding parameters are `protocols`, `local-ports` and `remote-ports` respectively.

Skip this step to protect all traffic between the ONTAP IP address and client IP address. Protecting all traffic is the default.

d. Enter the pre-shared key to use between the client and ONTAP.

Sample command

```
security ipsec policy create -vserver <vs1> -name <test34> -local-ip  
-subnets <192.168.134.34/32> -remote-ip-subnets <192.168.134.44/32>  
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```



IP traffic cannot flow between the client and server until the client pre-shared key is set on the IPsec client.

Use IPsec identities

Some IPsec clients, such as Libreswan, require the use of identities in addition to pre-shared keys to authenticate the IPsec connection.

About this task

Within ONTAP, identities are specified by modifying the SPD entry or during SPD policy creation. The SPD can be an IP address or string format identity name.

Step

To add an identity to an existing SPD, use the following command:

```
security ipsec policy modify
```

Sample command

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity  
192.168.134.34 -remote-identity client.fooboo.com
```

IPsec multiple client configuration

When a small number of clients need to leverage IPsec, using a single SPD entry for each client is sufficient. However, when hundreds or even thousands of clients need to leverage IPsec, NetApp recommends using an IPsec multiple client configuration.

About this task

ONTAP supports connecting multiple clients across many networks to a single SVM IP address with IPsec enabled. You can accomplish this using one of the following methods:

- **Subnet configuration**

To allow all clients on a particular subnet (192.168.134.0/24 for example) to connect to a single SVM IP address using a single SPD policy entry, you must specify the `remote-ip-subnets` in subnet form. Additionally, you must specify the `remote-identity` field with the correct client side identity.



When using a single policy entry in a subnet configuration, IPsec clients in that subnet share the IPsec identity and pre-shared key (PSK).

- **Allow all clients configuration**

To allow any client, regardless of their source IP address, to connect to the SVM IPsec-enabled IP address, use the `0.0.0.0/0` wild card when specifying the `remote-ip-subnets` field.

Additionally, you must specify the `remote-identity` field with the correct client side identity.

Also, when the `0.0.0.0/0` wild card is used, you must configure a specific local or remote port number to use. For example, `NFS port 2049`.

Step

1. Use one of the following commands to configure IPsec for multiple clients:

- a. If you are using a **subnet configuration** to support multiple IPsec clients:

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets  
IP_address/subnet -local-identity local_id -remote-identity remote_id
```

Sample command

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip  
-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local  
-identity ontap_side_identity -remote-identity client_side_identity
```

- b. If you are using an **allow all clients configuration** to support multiple IPsec clients:

```
security ipsec policy create -vserver vserver_name -name policy_name  
-local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local  
-ports port_number -local-identity local_id -remote-identity remote_id
```

Sample command

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
```

```
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local-identity ontap_side_identity -remote-identity client_side_identity
```

IPsec statistics

Through negotiation, a security channel called an IKE Security Association (SA) can be established between the ONTAP SVM IP address and the client IP address. IPsec SAs are installed on both endpoints to do the actual data encryption and decryption work.

You can use statistics commands to check the status of both IPsec SAs and IKE SAs.

Sample commands

IKE SA sample command:

```
security ipsec show-ikesasa -node hosting_node_name_for_svm_ip
```

IPsec SA sample command:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

Configure firewall policies for LIFs

Setting up a firewall enhances the security of the cluster and helps prevent unauthorized access to the storage system. By default, the firewall service allows remote systems access to a specific set of default services for data, management, and intercluster LIFs.

Firewall policies can be used to control access to management service protocols such as SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS, or SNMP. Firewall policies cannot be set for data protocols such as NFS or SMB/CIFS.

You can manage firewall service and policies in the following ways:

- Enabling or disabling firewall service
- Displaying the current firewall service configuration
- Creating a new firewall policy with the specified policy name and network services
- Applying a firewall policy to a logical interface
- Creating a new firewall policy that is an exact copy of an existing policy

You can use this to make a policy with similar characteristics within the same SVM, or to copy the policy to a different SVM.

- Displaying information about firewall policies
- Modifying the IP addresses and netmasks that are used by a firewall policy
- Deleting a firewall policy that is not being used by a LIF

Firewall policies and LIFs

LIF firewall policies are used to restrict access to the cluster over each LIF. You need to understand how the default firewall policy affects system access over each type of LIF, and how you can customize a firewall policy to increase or decrease security over a LIF.

When configuring a LIF using the `network interface create` or `network interface modify` command, the value specified for the `-firewall-policy` parameter determines the service protocols and IP addresses that are allowed access to the LIF.

In many cases you can accept the default firewall policy value. In other cases, you might need to restrict access to certain IP addresses and certain management service protocols. The available management service protocols include SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPs, RSH, DNS, and SNMP.

The firewall policy for all cluster LIFs defaults to `" "` and cannot be modified.

The following table describes the default firewall policies that are assigned to each LIF, depending on their role (ONTAP 9.5 and earlier) or service policy (ONTAP 9.6 and later), when you create the LIF:

Firewall policy	Default service protocols	Default access	LIFs applied to
mgmt	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Any address (0.0.0.0/0)	Cluster management, SVM management, and node management LIFs
mgmt-nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Any address (0.0.0.0/0)	Data LIFs that also support SVM management access
intercluster	https, ndmp, ndmps	Any address (0.0.0.0/0)	All intercluster LIFs
data	dns, ndmp, ndmps, portmap	Any address (0.0.0.0/0)	All data LIFs

Portmap service configuration

The portmap service maps RPC services to the ports on which they listen.

The portmap service was always accessible in ONTAP 9.3 and earlier, became configurable in ONTAP 9.4 through ONTAP 9.6, and is managed automatically starting in ONTAP 9.7.

- In ONTAP 9.3 and earlier, the portmap service (`rpcbind`) was always accessible on port 111 in network configurations that relied on the built-in ONTAP firewall rather than a third-party firewall.
- From ONTAP 9.4 through ONTAP 9.6, you can modify firewall policies to control whether the portmap service is accessible on particular LIFs.
- Starting in ONTAP 9.7, the portmap firewall service is eliminated. Instead, the portmap port is opened automatically for all LIFs that support the NFS service.

Portmap service is configurable in the firewall in ONTAP 9.4 through ONTAP 9.6.

The remainder of this topic discusses how to configure the portmap firewall service for ONTAP 9.4 through ONTAP 9.6 releases.

Depending on your configuration, you may be able to disallow access to the service on specific types of LIFs, typically management and intercluster LIFs. In some circumstances, you might even be able to disallow access on data LIFs.

What behavior you can expect

The ONTAP 9.4 through ONTAP 9.6 behavior is designed to provide a seamless transition on upgrade. If the portmap service is already being accessed over specific types of LIFs, it will continue to be accessible over those types of LIFs. As in previous ONTAP versions, you can specify the services accessible within the firewall in the firewall policy for the LIF type.

All nodes in the cluster must be running ONTAP 9.4 through ONTAP 9.6 for the behavior to take effect. Only inbound traffic is affected.

The new rules are as follows:

- * On upgrade to release 9.4 through 9.6, ONTAP adds the portmap service to all existing firewall policies, default or custom.
- * When you create a new cluster or new IPspace, ONTAP adds the portmap service only to the default data policy, not to the default management or intercluster policies.
- * You can add the portmap service to default or custom policies as needed, and remove the service as needed.

How to add or remove the portmap service

To add the portmap service to an SVM or cluster firewall policy (make it accessible within the firewall), enter:

```
system services firewall policy create -vserver SVM -policy mgmt|intercluster|data|custom -service portmap
```

To remove the portmap service from an SVM or cluster firewall policy (make it inaccessible within the firewall), enter:

```
system services firewall policy delete -vserver SVM -policy -policy mgmt|intercluster|data|custom -service portmap
```

You can use the network interface modify command to apply the firewall policy to an existing LIF. For complete command syntax, see [ONTAP 9 commands](#).

Create a firewall policy and assigning it to a LIF

Default firewall policies are assigned to each LIF when you create the LIF. In many cases, the default firewall settings work well and you do not need to change them. If you want to change the network services or IP addresses that can access a LIF, you can create a custom firewall policy and assign it to the LIF.

About this task

- You cannot create a firewall policy with the `policy` name `data`, `intercluster`, `cluster`, or `mgmt`.

These values are reserved for the system-defined firewall policies.

- You cannot set or modify a firewall policy for cluster LIFs.

The firewall policy for cluster LIFs is set to 0.0.0.0/0 for all services types.

- If you need to modify or remove services, you must delete the existing firewall policy and create a new policy.
- If IPv6 is enabled on the cluster, you can create firewall policies with IPv6 addresses.

After IPv6 is enabled, `data` and `mgmt` firewall policies include ::/0, the IPv6 wildcard, in their list of accepted addresses.

- When using ONTAP System Manager to configure data protection functionality across clusters, you must ensure that the intercluster LIF IP addresses are included in the allowed list, and that HTTPS service is allowed on both the intercluster LIFs and on your company-owned firewalls.

By default, the `intercluster` firewall policy allows access from all IP addresses (0.0.0.0/0) and enables HTTPS, NDMP, and NDMPS services. If you modify this default policy, or if you create your own firewall policy for intercluster LIFs, you must add each intercluster LIF IP address to the allowed list and enable HTTPS service.

- Starting with ONTAP 9.6, the HTTPS and SSH firewall services are not supported.

In ONTAP 9.6, the `management-https` and `management-ssh` LIF services are available for HTTPS and SSH management access.

Steps

- Create a firewall policy that will be available to the LIFs on a specific SVM:

```
system services firewall policy create -vserver vserver_name -policy policy_name -service network_service -allow-list ip_address/mask
```

You can use this command multiple times to add more than one network service and list of allowed IP addresses for each service in the firewall policy.

- Verify that the policy was added correctly by using the `system services firewall policy show` command.
- Apply the firewall policy to a LIF:

```
network interface modify -vserver vserver_name -lif lif_name -firewall-policy policy_name
```

- Verify that the policy was added correctly to the LIF by using the `network interface show -fields firewall-policy` command.

Example of creating a firewall policy and applying it to a LIF

The following command creates a firewall policy named `data_http` that enables HTTP and HTTPS protocol access from IP addresses on the 10.10 subnet, applies that policy to the LIF named `data1` on SVM `vs1`, and then shows all of the firewall policies on the cluster:

```
system services firewall policy create -vserver vs1 -policy data_http -service http -allow-list 10.10.0.0/16
```

```

system services firewall policy show

Vserver Policy      Service      Allowed
----- -----
cluster-1
    data
        dns          0.0.0.0/0
        ndmp         0.0.0.0/0
        ndmps        0.0.0.0/0
cluster-1
    intercluster
        https        0.0.0.0/0
        ndmp         0.0.0.0/0
        ndmps        0.0.0.0/0
cluster-1
    mgmt
        dns          0.0.0.0/0
        http         0.0.0.0/0
        https        0.0.0.0/0
        ndmp         0.0.0.0/0
        ndmps        0.0.0.0/0
        ntp          0.0.0.0/0
        snmp         0.0.0.0/0
        ssh          0.0.0.0/0
vs1
    data_http
        http         10.10.0.0/16
        https        10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
----- -----
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt       mgmt
cluster-1 node1_mgmt1       mgmt
cluster-1 node2_mgmt1       mgmt
vs1      data1                data_http
vs3      data2                data

```

Commands for managing firewall service and policies

You can use the `system services firewall` commands to manage firewall service, the `system services firewall policy` commands to manage firewall policies, and the `network interface modify` command to manage firewall settings for LIFs.

If you want to...	Use this command...
Enable or disable firewall service	<code>system services firewall modify</code>
Display the current configuration for firewall service	<code>system services firewall show</code>
Create a firewall policy or add a service to an existing firewall policy	<code>system services firewall policy create</code>
Apply a firewall policy to a LIF	<code>network interface modify -lif lifname - firewall-policy</code>
Modify the IP addresses and netmasks associated with a firewall policy	<code>system services firewall policy modify</code>
Display information about firewall policies	<code>system services firewall policy show</code>
Create a new firewall policy that is an exact copy of an existing policy	<code>system services firewall policy clone</code>
Delete a firewall policy that is not used by a LIF	<code>system services firewall policy delete</code>

For more information, see the man pages for the `system services firewall`, `system services firewall policy`, and `network interface modify` commands in [ONTAP 9 commands](#).

Configure QoS marking (cluster administrators only)

Overview

Network Quality of Service (QoS) marking helps you to prioritize different traffic types based on the network conditions to effectively utilize the network resources. You can set the differentiated services code point (DSCP) value of the outgoing IP packets for the supported traffic types per IPspace.

DSCP marking for UC compliance

You can enable differentiated services code point (DSCP) marking on outgoing (egress) IP packet traffic for a given protocol with a default or user-provided DSCP code. DSCP marking is a mechanism for classifying and managing network traffic and is a component of Unified Capability (UC) compliance.

DSCP marking (also known as *QoS marking* or *quality of service marking*) is enabled by providing an IPspace, protocol, and DSCP value. The protocols on which DSCP marking can be applied are NFS, CIFS, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet, and SNMP.

If you do not provide a DSCP value when enabling DSCP marking for a given protocol, a default is used:

- The default value for data protocols/traffic is 0x0A (10).
- The default value for control protocols/traffic is 0x30 (48).

Modify QoS marking values

You can modify the Quality of Service (QoS) marking values for different protocols, for each IPspace.

Before you begin

All nodes in the cluster must be running the same version of ONTAP.

Step

Modify QoS marking values by using the `network qos-marking modify` command.

- The `-ipspace` parameter specifies the IPspace for which the QoS marking entry is to be modified.
- The `-protocol` parameter specifies the protocol for which the QoS marking entry is to be modified. The `network qos-marking modify` man page describes the possible values of the protocol.
- The `-dscp` parameter specifies the Differentiated Services Code Point (DSCP) value. The possible values ranges from 0 through 63.
- The `-is-enabled` parameter is used to enable or disable the QoS marking for the specified protocol in the IPspace provided by the `-ipspace` parameter.

The following command enables the QoS marking for the NFS protocol in default IPspace:

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

The following command sets the DSCP value to 20 for the NFS protocol in the default IPspace:

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

Display QoS marking values

You can display the QoS marking values for different protocols, for each IPspace.

Step

Display QoS marking values by using the `network qos-marking show` command.

The following command displays the QoS marking for all protocols in the default IPspace:

```

network qos-marking show -ipspace Default
IPspace          Protocol        DSCP   Enabled?
-----
Default
      CIFS           10   false
      FTP            48   false
      HTTP-admin     48   false
      HTTP-filesrv  10   false
      NDMP           10   false
      NFS            10   true
      SNMP           48   false
      SSH            48   false
      SnapMirror    10   false
      Telnet         48   false
      iSCSI          10   false
11 entries were displayed.

```

Manage SNMP on the cluster (cluster administrators only)

Overview

You can configure SNMP to monitor SVMs in your cluster to avoid issues before they occur, and to respond to issues if they do occur. Managing SNMP involves configuring SNMP users and configuring SNMP traphost destinations (management workstations) for all SNMP events. SNMP is disabled by default on data LIFs.

You can create and manage read-only SNMP users in the data SVM. Data LIFs must be configured to receive SNMP requests on the SVM.

SNMP network management workstations, or managers, can query the SVM SNMP agent for information. The SNMP agent gathers information and forwards it to the SNMP managers. The SNMP agent also generates trap notifications whenever specific events occur. The SNMP agent on the SVM has read-only privileges; it cannot be used for any set operations or for taking a corrective action in response to a trap. ONTAP provides an SNMP agent compatible with SNMP versions v1, v2c, and v3. SNMPv3 offers advanced security by using passphrases and encryption.

For more information about SNMP support in ONTAP systems, see [TR-4220: SNMP Support in Data ONTAP](#).

What MIBs are

A MIB (Management Information Base) is a text file that describes SNMP objects and traps.

MIBs describe the structure of the management data of the storage system and they use a hierarchical namespace containing object identifiers (OIDs). Each OID identifies a variable that can be read by using SNMP.

Because MIBs are not configuration files and ONTAP does not read these files, SNMP functionality is not

affected by MIBs. ONTAP provides the following MIB file:

- A NetApp custom MIB ([netapp.mib](#))

ONTAP supports IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113), and ICMP (RFC 2466) MIBs, which show both IPv4 and IPv6 data, are supported.

ONTAP also provides a short cross-reference between object identifiers (OIDs) and object short names in the [traps.dat](#) file.



The latest versions of the ONTAP MIBs and `traps.dat` files are available on the NetApp Support Site. However, the versions of these files on the support site do not necessarily correspond to the SNMP capabilities of your ONTAP version. These files are provided to help you evaluate SNMP features in the latest ONTAP version.

SNMP traps

SNMP traps capture system monitoring information that is sent as an asynchronous notification from the SNMP agent to the SNMP manager.

There are three types of SNMP traps: standard, built-in, and user-defined. User-defined traps are not supported in ONTAP.

A trap can be used to check periodically for operational thresholds or failures that are defined in the MIB. If a threshold is reached or a failure is detected, the SNMP agent sends a message (trap) to the traphosts alerting them of the event.



ONTAP supports SNMPv1 traps and, starting in ONTAP 9.1, SNMPv3 traps. ONTAP does not support SNMPv2c traps and INFORMs.

Standard SNMP traps

These traps are defined in RFC 1215. There are five standard SNMP traps that are supported by ONTAP: coldStart, warmStart, linkDown, linkUp, and authenticationFailure.



The authenticationFailure trap is disabled by default. You must use the [system snmp authtrap](#) command to enable the trap. For more information, see the man pages: [ONTAP 9 commands](#)

Built-in SNMP traps

Built-in traps are predefined in ONTAP and are automatically sent to the network management stations on the traphost list if an event occurs. These traps, such as diskFailedShutdown, cpuTooBusy, and volumeNearlyFull, are defined in the custom MIB.

Each built-in trap is identified by a unique trap code.

Create an SNMP community and assigning it to a LIF

You can create an SNMP community that acts as an authentication mechanism between the management station and the storage virtual machine (SVM) when using SNMPv1 and SNMPv2c.

By creating SNMP communities in a data SVM, you can execute commands such as `snmpwalk` and `snmpget` on the data LIFs.

About this task

- In new installations of ONTAP, SNMPv1 and SNMPv2c are disabled by default.
- SNMPv1 and SNMPv2c are enabled after you create an SNMP community.
- ONTAP supports read-only communities.
- By default, the "data" firewall policy that is assigned to data LIFs has SNMP service set to `deny`.

You must create a new firewall policy with SNMP service set to `allow` when creating an SNMP user for a data SVM.

- You can create SNMP communities for SNMPv1 and SNMPv2c users for both the admin SVM and the data SVM.
- Because an SVM is not part of the SNMP standard, queries on data LIFs must include the NetApp root OID (1.3.6.1.4.1.789)—for example, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Steps

1. Create an SNMP community by using the `system snmp community add` command. The following command shows how to create an SNMP community in the admin SVM cluster-1:

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

The following command shows how to create an SNMP community in the data SVM vs1:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verify that the communities have been created by using the `system snmp community show` command.

The following command shows the two communities created for SNMPv1 and SNMPv2c:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Check whether SNMP is allowed as a service in the "data" firewall policy by using the `system services firewall policy show` command.

The following command shows that the snmp service is not allowed in the default "data" firewall policy (the snmp service is allowed in the "mgmt" firewall policy only):

```

system services firewall policy show
Vserver Policy      Service     Allowed
-----
cluster-1
    data
        dns          0.0.0.0/0
        ndmp         0.0.0.0/0
        ndmps        0.0.0.0/0
cluster-1
    intercluster
        https        0.0.0.0/0
        ndmp         0.0.0.0/0
        ndmps        0.0.0.0/0
cluster-1
    mgmt
        dns          0.0.0.0/0
        http         0.0.0.0/0
        https        0.0.0.0/0
        ndmp         0.0.0.0/0
        ndmps        0.0.0.0/0
        ntp          0.0.0.0/0
        snmp         0.0.0.0/0
        ssh          0.0.0.0/0

```

4. Create a new firewall policy that allows access using the `snmp` service by using the `system services firewall policy create` command.

The following commands create a new data firewall policy named "data1" that allows the `snmp`

```

system services firewall policy create -policy data1 -service snmp
-vserver vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver Policy      Service     Allowed
-----
cluster-1
    mgmt
        snmp        0.0.0.0/0
vs1
    data1
        snmp        0.0.0.0/0

```

5. Apply the firewall policy to a data LIF by using the `network interface modify` command with the `-firewall-policy` parameter.

The following command assigns the new "data1" firewall policy to LIF "datalif1":

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy  
data1
```

Configure SNMPv3 users in a cluster

SNMPv3 is a secure protocol when compared to SNMPv1 and SNMPv2c. To use SNMPv3, you must configure an SNMPv3 user to run the SNMP utilities from the SNMP manager.

Step

Use the "security login create command" to create an SNMPv3 user.

You are prompted to provide the following information:

- Engine ID: Default and recommended value is local Engine ID
- Authentication protocol
- Authentication password
- Privacy protocol
- Privacy protocol password

Result

The SNMPv3 user can log in from the SNMP manager by using the user name and password and run the SNMP utility commands.

SNMPv3 security parameters

SNMPv3 includes an authentication feature that, when selected, requires users to enter their names, an authentication protocol, an authentication key, and their desired security level when invoking a command.

The following table lists the SNMPv3 security parameters :

Parameter	Command-line option	Description
engineID	-e EngineID	Engine ID of the SNMP agent. Default value is local EngineID (recommended).
securityName	-u Name	User name must not exceed 32 characters.
authProtocol	-a {none MD5 SHA SHA-256}	Authentication type can be none, MD5, SHA, or SHA-256.
authKey	-A PASSPHRASE	Passphrase with a minimum of eight characters.

Parameter	Command-line option	Description
securityLevel	-l {authNoPriv AuthPriv noAuthNoPriv}	Security level can be Authentication, No Privacy; Authentication, Privacy; or no Authentication, no Privacy.
privProtocol	-x { none des aes128}	Privacy protocol can be none, des, or aes128
privPassword	-X password	Password with a minimum of eight characters.

Examples for different security levels

This example shows how an SNMPv3 user created with different security levels can use the SNMP client-side commands, such as `snmpwalk`, to query the cluster objects.

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.



You must use `snmpwalk` 5.3.1 or later when the authentication protocol is SHA.

Security level: authPriv

The following output shows the creation of an SNMPv3 user with the authPriv security level.

```
security login create -username snmpv3user -application snmp -authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]:sha
```

FIPS mode

```
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (none, des) [none]: des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk Test

The following output shows the SNMPv3 user running the `snmpwalk` command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Security level: authNoPriv

The following output shows the creation of an SNMPv3 user with the authNoPriv security level.

```
security login create -username snmpv3user1 -application snmp -authmethod usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS Mode

```
Which privacy protocol do you want to choose (aes128) [aes128]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (none, des) [none]: none
```

snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1! -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Security level: noAuthNoPriv

The following output shows the creation of an SNMPv3 user with the noAuthNoPriv security level.

```
security login create -username snmpv3user2 -application snmp -authmethod usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS Mode

FIPS will not allow you to choose none

snmpwalk Test

The following output shows the SNMPv3 user running the snmpwalk command:

For better performance, you should retrieve all objects in a table rather than a single object or a few objects from the table.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Configure traphosts to receive SNMP notifications

You can configure the traphost (SNMP manager) to receive notifications (SNMP trap PDUs) when SNMP traps are generated in the cluster. You can specify either the host name or the IP address (IPv4 or IPv6) of the SNMP traphost.

Before you begin

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



SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster for resolving the traphost names.
- IPv6 must be enabled on the cluster to configure SNMP traphosts by using IPv6 addresses.
- For ONTAP 9.1 and later versions, you must have specified the authentication of a predefined User-based Security Model (USM) and privacy credentials when creating traphosts.

Step

Add an SNMP traphost:

```
system snmp traphost add
```



Traps can be sent only when at least one SNMP management station is specified as a traphost.

The following command adds a new SNMPv3 traphost named `yyy.example.com` with a known USM user:

```
system snmp traphost add -peer-address yyy.example.com -usm-username  
MyUsmUser
```

The following command adds a traphost using the IPv6 address of the host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Commands for managing SNMP

You can use the `system snmp` commands to manage SNMP, traps, and traphosts. You can use the `security` commands to manage SNMP users per SVM. You can use the `event` commands to manage events related to SNMP traps.

Commands for configuring SNMP

If you want to...	Use this command...
Enable SNMP on the cluster	<code>options -option-name snmp.enable -option- value on</code> The SNMP service must be allowed under the management (mgmt) firewall policy. You can verify whether SNMP is allowed by using the <code>system services firewall policy show</code> command.
Disable SNMP on the cluster	<code>options -option-name snmp.enable -option- value off</code>

Commands for managing SNMP v1, v2c, and v3 users

If you want to...	Use this command...
Configure SNMP users	<code>security login create</code>
Display SNMP users	<code>security snmpusers</code> and <code>security login show -application snmp</code>
Delete SNMP users	<code>security login delete</code>
Modify the access-control role name of a login method for SNMP users	<code>security login modify</code>

Commands for providing contact and location information

If you want to...	Use this command...
Display or modify the contact details of the cluster	System snmp contact
Display or modify the location details of the cluster	System snmp location

Commands for managing SNMP communities

If you want to...	Use this command...
Add a read-only (ro) community for an SVM or for all SVMs in the cluster	system snmp community add
Delete a community or all communities	system snmp community delete
Display the list of all communities	system snmp community show

Because SVMs are not part of the SNMP standard, queries on data LIFs must include the NetApp root OID (1.3.6.1.4.1.789), for example, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Command for displaying SNMP option values

If you want to...	Use this command...
Display the current values of all SNMP options, including cluster contact, contact location, whether the cluster is configured to send traps, the list of traphosts, and list of communities and access control type	system snmp show

Commands for managing SNMP traps and traphosts

If you want to...	Use this command...
Enable SNMP traps sent from the cluster	system snmp init -init 1
Disable SNMP traps sent from the cluster	system snmp init -init 0
Add a traphost that receives SNMP notifications for specific events in the cluster	system snmp traphost add
Delete a traphost	system snmp traphost delete
Display the list of traphosts	system snmp traphost show

Commands for managing events related to SNMP traps

If you want to...	Use this command...
Display the events for which SNMP traps (built-in) are generated	<p>event route show</p> <p>Use the -snmp-support true parameter to view only SNMP-related events.</p> <p>Use the instance -messagename <message> parameter to view a detailed description why an event might have occurred, and any corrective action.</p> <p>Routing of individual SNMP trap events to specific traphost destinations is not supported. All SNMP trap events are sent to all traphost destinations.</p>
Display a list of SNMP trap history records, which are event notifications that have been sent to SNMP traps	event snmphistory show
Delete an SNMP trap history record	event snmphistory delete

For more information about the `system snmp`, `security`, and `event` commands, see the man pages: [ONTAP 9 commands](#)

Manage routing in an SVM

Overview

The routing table for an SVM determines the network path the SVM uses to communicate with a destination. It's important to understand how routing tables work so that you can prevent network problems before they occur.

Routing rules are as follows:

- ONTAP routes traffic over the most specific available route.
- ONTAP routes traffic over a default gateway route (having 0 bits of netmask) as a last resort, when more specific routes are not available.

In the case of routes with the same destination, netmask, and metric, there is no guarantee that the system will use the same route after a reboot or after an upgrade. This is especially an issue if you have configured multiple default routes.

It is a best practice to configure one default route only for an SVM. To avoid disruption, you should ensure that the default route is able to reach any network address that is not reachable by a more specific route. For more information, see the Knowledgebase article [SU134: Network access might be disrupted by incorrect routing configuration in clustered ONTAP](#)

Create a static route

You can create static routes within a storage virtual machine (SVM) to control how LIFs use the network for outbound traffic.

When you create a route entry associated with an SVM, the route will be used by all LIFs that are owned by the specified SVM and that are on the same subnet as the gateway.

Step

Use the `network route create` command to create a route.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway  
10.61.208.1
```

Enable multipath routing

If multiple routes have the same metric for a destination, only one of the routes is picked for outgoing traffic. This leads to other routes being unutilized for sending outgoing traffic. You can enable multipath routing to load balance and utilize all the available routes.

Steps

1. Log in to the advanced privilege level:

```
set -privilege advanced
```

2. Enable multipath routing:

```
network options multipath-routing modify -is-enabled true
```

Multipath routing is enabled for all nodes in the cluster.

```
network options multipath-routing modify -is-enabled true
```

Delete a static route

You can delete an unneeded static route from a storage virtual machine (SVM).

Step

Use the `network route delete` command to delete a static route.

For more information about this command, see the `network route` man page: [ONTAP 9 commands](#).

The following example deletes a static route associated with SVM vs0 with a gateway of 10.63.0.1 and a destination IP address of 0.0.0.0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination  
0.0.0.0/0
```

Display routing information

You can display information about the routing configuration for each SVM on your cluster.

This can help you diagnose routing problems involving connectivity issues between client applications or services and a LIF on a node in the cluster.

Steps

1. Use the `network route show` command to display routes within one or more SVMs. The following example shows a route configured in the vs0 SVM:

```
network route show
(network route show)
Vserver          Destination      Gateway        Metric
-----
vs0              0.0.0.0/0       172.17.178.1   20
```

2. Use the `network route show-lifs` command to display the association of routes and LIFs within one or more SVMs.

The following example shows LIFs with routes owned by the vs0 SVM:

```
network route show-lifs
(network route show-lifs)

Vserver: vs0
Destination          Gateway           Logical Interfaces
-----
0.0.0.0/0            172.17.178.1    cluster_mgmt,
                           LIF-b-01_mgmt1,
                           LIF-b-02_mgmt1
```

3. Use the `network route active-entry show` command to display installed routes on one or more nodes, SVMs, subnets, or routes with specified destinations.

The following example shows all installed routes on a specific SVM:

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination          Gateway           Interface  Metric  Flags
-----
127.0.0.1            127.0.0.1         lo        10      UHS
127.0.10.1           127.0.20.1        losk      10      UHS
127.0.20.1           127.0.20.1        losk      10      UHS
```

```

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination           Gateway             Interface   Metric  Flags
-----
default              fd20:8b1e:b255:814e::1      e0d        20      UGS
fd20:8b1e:b255:814e::/64
                    link#4            e0d        0       UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination           Gateway             Interface   Metric  Flags
-----
127.0.0.1            127.0.0.1          lo         10      UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination           Gateway             Interface   Metric  Flags
-----
127.0.10.1           127.0.20.1         losk       10      UHS
127.0.20.1           127.0.20.1         losk       10      UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination           Gateway             Interface   Metric  Flags
-----
default              fd20:8b1e:b255:814e::1      e0d        20      UGS
fd20:8b1e:b255:814e::/64
                    link#4            e0d        0       UC
fd20:8b1e:b255:814e::1 link#4            e0d        0       UHL
11 entries were displayed.

```

Remove dynamic routes from routing tables

When ICMP redirects are received for IPv4 and IPv6, dynamic routes are added to the routing table. By default, the dynamic routes are removed after 300 seconds. If you want to maintain dynamic routes for a different amount of time, you can change the time out value.

About this task

You can set the timeout value from 0 to 65,535 seconds. If you set the value to 0, the routes never expire.

Removing dynamic routes prevents loss of connectivity caused by the persistence of invalid routes.

Steps

1. Display the current timeout value.

- For IPv4:

```
network tuning icmp show
```

- For IPv6:

```
network tuning icmp6 show
```

2. Modify the timeout value.

- For IPv4:

```
network tuning icmp modify -node node_name -redirect-timeout  
timeout_value
```

- For IPv6:

```
network tuning icmp6 modify -node node_name -redirect-v6-timeout  
timeout_value
```

3. Verify that the timeout value was modified correctly.

- For IPv4:

```
network tuning icmp show
```

- For IPv6:

```
network tuning icmp6 show
```

ONTAP port usage on a storage system

Overview

A number of well-known ports are reserved for ONTAP communications with specific services. Port conflicts will occur if a port value in your storage network environment is the same as on ONTAP port.

Network Ports

The following table lists the TCP ports and UDP ports that are used by ONTAP.

Service	Port/Protocol	Description
ssh	22/TCP	Secure shell login
telnet	23/TCP	Remote login
DNS	53/TCP	Load Balanced DNS
http	80/TCP	Hyper Text Transfer Protocol
rpcbind	111/TCP	Remote procedure call
rpcbind	111/UDP	Remote procedure call
ntp	123/UDP	Network Time Protocol
msrpc	135/UDP	MSRPC
netbios-ssn	139/TCP	NetBIOS service session
snmp	161/UDP	Simple network management protocol
https	443/TCP	HTTP over TLS
microsoft-ds	445/TCP	Microsoft-ds
mount	635/TCP	NFS mount
mount	635/UDP	NFS Mount
named	953/UDP	Name daemon
nfs	2049/UDP	NFS Server daemon
nfs	2049/TCP	NFS Server daemon
nrv	2050/TCP	NetApp Remote Volume protocol
iscsi	3260/TCP	iSCSI target port
lockd	4045/TCP	NFS lock daemon
lockd	4045/UDP	NFS lock daemon
NFS	4046/TCP	Network Status Monitor
NSM	4046/UDP	Network Status Monitor
rquotad	4049/UDP	NFS rquotad protocol
krb524	4444/UDP	Kerberos 524
mdns	5353/UDP	Multicast DNS
HTTPS	5986/UDP	HTTPS Port - Listening binary protocol
https	8443/TCP	7MTT GUI Tool through https
ndmp	10000/TCP	Network Data Management Protocol

Service	Port/Protocol	Description
Cluster peering	11104/TCP	Cluster peering
Cluster peering	11105/TCP	Cluster peering
NDMP	18600 - 18699/TCP	NDMP
cifs witness port	40001/TCP	cifs witness port
tls	50000/TCP	Transport layer security
iscsi	65200/TCP	ISCSI port

ONTAP internal ports

The following table lists the TCP ports and UDP ports that are used internally by ONTAP. These ports are used to establish intracluster LIF communication:

Port/Protocol	Description
514	Syslog
900	NetApp Cluster RPC
902	NetApp Cluster RPC
904	NetApp Cluster RPC
905	NetApp Cluster RPC
910	NetApp Cluster RPC
911	NetApp Cluster RPC
913	NetApp Cluster RPC
914	NetApp Cluster RPC
915	NetApp Cluster RPC
918	NetApp Cluster RPC
920	NetApp Cluster RPC
921	NetApp Cluster RPC
924	NetApp Cluster RPC
925	NetApp Cluster RPC
927	NetApp Cluster RPC
928	NetApp Cluster RPC
929	NetApp Cluster RPC
931	NetApp Cluster RPC
932	NetApp Cluster RPC
933	NetApp Cluster RPC
934	NetApp Cluster RPC

Port/Protocol	Description
935	NetApp Cluster RPC
936	NetApp Cluster RPC
937	NetApp Cluster RPC
939	NetApp Cluster RPC
940	NetApp Cluster RPC
951	NetApp Cluster RPC
954	NetApp Cluster RPC
955	NetApp Cluster RPC
956	NetApp Cluster RPC
958	NetApp Cluster RPC
961	NetApp Cluster RPC
963	NetApp Cluster RPC
964	NetApp Cluster RPC
966	NetApp Cluster RPC
967	NetApp Cluster RPC
5125	Alternate Control Port for disk
5133	Alternate Control Port for disk
5144	Alternate Control Port for disk
65502	Node scope SSH
65503	LIF Sharing
7810	NetApp Cluster RPC
7811	NetApp Cluster RPC
7812	NetApp Cluster RPC
7813	NetApp Cluster RPC
7814	NetApp Cluster RPC
7815	NetApp Cluster RPC
7816	NetApp Cluster RPC
7817	NetApp Cluster RPC
7818	NetApp Cluster RPC
7819	NetApp Cluster RPC
7820	NetApp Cluster RPC
7821	NetApp Cluster RPC
7822	NetApp Cluster RPC

Port/Protocol	Description
7823	NetApp Cluster RPC
7824	NetApp Cluster RPC
8023	Node Scope TELNET
8514	Node Scope RSH
9877	KMIP Client Port (Internal Local Host Only)

View network information

Overview

You can view information related to ports, LIFs, routes, failover rules, failover groups, firewall rules, DNS, NIS, and connections.

This information can be useful in situations such as reconfiguring networking settings, or when troubleshooting the cluster.

If you are a cluster administrator, you can view all the available networking information. If you are an SVM administrator, you can view only the information related to your assigned SVMs.

Display network port information (cluster administrators only)

You can display information about a specific port, or about all ports on all nodes in the cluster.

About this task

The following information is displayed:

- Node name
- Port name
- IPspace name
- Broadcast domain name
- Link status (up or down)
- MTU setting
- Port speed setting and operational status (1 gigabit or 10 gigabits per second)
- Auto-negotiation setting (true or false)
- Duplex mode and operational status (half or full)
- The port's interface group, if applicable
- The port's VLAN tag information, if applicable
- The port's health status (health or degraded)
- Reasons for a port being marked as degraded

If data for a field is not available (for example, the operational duplex and speed for an inactive port would not be available), the field value is listed as **-**.

Step

Display network port information by using the `network port show` command.

You can display detailed information for each port by specifying the `-instance` parameter, or get specific information by specifying field names using the `-fields` parameter.

```
network port show
Node: node1

Ignore                                                 Speed (Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper Status
Status

-----
-----
```

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/1000	healthy
false							
e0b	Cluster	Cluster		up	9000	auto/1000	healthy
false							
e0c	Default	Default		up	1500	auto/1000	degraded
false							
e0d	Default	Default		up	1500	auto/1000	degraded
true							

```
Node: node2

Ignore                                                 Speed (Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper Status
Status

-----
-----
```

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
e0a	Cluster	Cluster		up	9000	auto/1000	healthy
false							
e0b	Cluster	Cluster		up	9000	auto/1000	healthy
false							
e0c	Default	Default		up	1500	auto/1000	healthy
false							
e0d	Default	Default		up	1500	auto/1000	healthy
false							

```
8 entries were displayed.
```

Display information about a VLAN (cluster administrators only)

You can display information about a specific VLAN or about all VLANs in the cluster.

About this task

You can display detailed information for each VLAN by specifying the `-instance` parameter. You can display specific information by specifying field names using the `-fields` parameter.

Step

Display information about VLANs by using the `network port vlan show` command. The following command displays information about all VLANs in the cluster:

```
network port vlan show
      Network Network
Node   VLAN Name Port     VLAN ID MAC Address
----- -----
cluster-1-01
    a0a-10    a0a     10    02:a0:98:06:10:b2
    a0a-20    a0a     20    02:a0:98:06:10:b2
    a0a-30    a0a     30    02:a0:98:06:10:b2
    a0a-40    a0a     40    02:a0:98:06:10:b2
    a0a-50    a0a     50    02:a0:98:06:10:b2
cluster-1-02
    a0a-10    a0a     10    02:a0:98:06:10:ca
    a0a-20    a0a     20    02:a0:98:06:10:ca
    a0a-30    a0a     30    02:a0:98:06:10:ca
    a0a-40    a0a     40    02:a0:98:06:10:ca
    a0a-50    a0a     50    02:a0:98:06:10:ca
```

Display interface group information (cluster administrators only)

You can display information about an interface group to determine its configuration.

About this task

The following information is displayed:

- Node on which the interface group is located
- List of network ports that are included in the interface group
- Interface group's name
- Distribution function (MAC, IP, port, or sequential)
- Interface group's Media Access Control (MAC) address
- Port activity status; that is, whether all aggregated ports are active (full participation), whether some are active (partial participation), or whether none are active

Step

Display information about interface groups by using the `network port ifgrp show` command.

You can display detailed information for each node by specifying the `-instance` parameter. You can display specific information by specifying field names using the `-fields` parameter.

The following command displays information about all interface groups in the cluster:

network port ifgrp show					
Node	Port IfGrp	Distribution Function	MAC Address	Active	
				Ports	Ports
<hr/>					
cluster-1-01	a0a	ip	02:a0:98:06:10:b2	full	e7a, e7b
cluster-1-02	a0a	sequential	02:a0:98:06:10:ca	full	e7a, e7b
cluster-1-03	a0a	port	02:a0:98:08:5b:66	full	e7a, e7b
cluster-1-04	a0a	mac	02:a0:98:08:61:4e	full	e7a, e7b

The following command displays detailed interface group information for a single node:

```
network port ifgrp show -instance -node cluster-1-01

          Node: cluster-1-01
Interface Group Name: a0a
Distribution Function: ip
          Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
Port Participation: full
          Network Ports: e7a, e7b
          Up Ports: e7a, e7b
          Down Ports: -
```

Display LIF information

You can view detailed information about a LIF to determine its configuration.

You might also want to view this information to diagnose basic LIF problems, such as checking for duplicate IP addresses or verifying whether the network port belongs to the correct subnet. storage virtual machine (SVM) administrators can view only the information about the LIFs associated with the SVM.

About this task

The following information is displayed:

- IP address associated with the LIF
- Administrative status of the LIF

- Operational status of the LIF

The operational status of data LIFs is determined by the status of the SVM with which the data LIFs are associated. When the SVM is stopped, the operational status of the LIF changes to down. When the SVM is started again, the operational status changes to up

- Node and the port on which the LIF resides

If data for a field is not available (for example, if there is no extended status information), the field value is listed as **-**.

Step

Display LIF information by using the network interface show command.

You can view detailed information for each LIF by specifying the **-instance** parameter, or get specific information by specifying field names using the **-fields** parameter.

The following command displays general information about all LIFs in a cluster:

```

network interface show
  Logical      Status      Network          Current       Current Is
Vserver     Interface   Admin/Oper Address/Mask    Node        Port
Home

-----
-----

example
  lif1         up/up      192.0.2.129/22    node-01
                                         e0d
false
node
  cluster_mgmt up/up      192.0.2.3/20      node-02
                                         e0c
false
node-01
  clus1        up/up      192.0.2.65/18     node-01
                                         e0a
true
  clus2        up/up      192.0.2.66/18     node-01
                                         e0b
true
  mgmt1        up/up      192.0.2.1/20      node-01
                                         e0c
true
node-02
  clus1        up/up      192.0.2.67/18     node-02
                                         e0a
true
  clus2        up/up      192.0.2.68/18     node-02
                                         e0b
true
  mgmt2        up/up      192.0.2.2/20      node-02
                                         e0d
true
vs1
  d1           up/up      192.0.2.130/21    node-01
                                         e0d
false
  d2           up/up      192.0.2.131/21    node-01
                                         e0d
true
  data3        up/up      192.0.2.132/20    node-02
                                         e0c
true

```

The following command shows detailed information about a single LIF:

```
network interface show -lif data1 -instance

          Vserver Name: vs1
          Logical Interface Name: data1
          Role: data
          Data Protocol: nfs,cifs
          Home Node: node-01
          Home Port: e0c
          Current Node: node-03
          Current Port: e0c
          Operational Status: up
          Extended Status: -
          Is Home: false
          Network Address: 192.0.2.128
          Netmask: 255.255.192.0
          Bits in the Netmask: 18
          IPv4 Link Local: -
          Subnet Name: -
          Administrative Status: up
          Failover Policy: local-only
          Firewall Policy: data
          Auto Revert: false
          Fully Qualified DNS Zone Name: xxx.example.com
          DNS Query Listen Enable: false
          Failover Group Name: Default
          FCP WWPN: -
          Address family: ipv4
          Comment: -
          IPspace of LIF: Default
```

Display routing information

You can display information about routes within an SVM.

Step

Depending on the type of routing information that you want to view, enter the applicable command:

To view information about...	Enter
Static routes, per SVM	<code>network route show</code>
LIFs on each route, per SVM	<code>network route show-lifs</code>

You can display detailed information for each route by specifying the `-instance` parameter. The following command displays the static routes within the SVMs in cluster-1:

```

network route show
Vserver           Destination      Gateway        Metric
-----
Cluster          0.0.0.0/0       10.63.0.1     10
cluster-1        0.0.0.0/0       198.51.9.1    10
vs1              0.0.0.0/0       192.0.2.1     20
vs3              0.0.0.0/0       192.0.2.1     20

```

The following command displays the association of static routes and logical interfaces (LIFs) within all SVMs in cluster-1:

```

network route show-lifs
Vserver: Cluster
Destination      Gateway        Logical Interfaces
-----
0.0.0.0/0       10.63.0.1     -
Vserver: cluster-1
Destination      Gateway        Logical Interfaces
-----
0.0.0.0/0       198.51.9.1   cluster_mgmt,
                           cluster-1_mgmt1,
Vserver: vs1
Destination      Gateway        Logical Interfaces
-----
0.0.0.0/0       192.0.2.1    data1_1, data1_2
Vserver: vs3
Destination      Gateway        Logical Interfaces
-----
0.0.0.0/0       192.0.2.1    data2_1, data2_2

```

Display DNS host table entries (cluster administrators only)

The DNS host table entries map host names to IP addresses. You can display the host names and alias names and the IP address that they map to for all SVMs in a cluster.

Step

Display the host name entries for all SVMs by using the vserver services name-service dns hosts show command.

The following example displays the host table entries:

```
vserver services name-service dns hosts show
Vserver      Address          Hostname        Aliases
-----
cluster-1
vs1          10.72.219.36    lnx219-36      -
vs1          10.72.219.37    lnx219-37      lnx219-37.example.com
```

You can use the `vserver services name-service dns` command to enable DNS on an SVM, and configure it to use DNS for host-name resolution. Host names are resolved using external DNS servers.

Display DNS domain configurations

You can display the DNS domain configuration of one or more storage virtual machines (SVMs) in your cluster to verify that it is configured properly.

Step

Viewing the DNS domain configurations by using the `vserver services name-service dns show` command.

The following command displays the DNS configurations for all SVMs in the cluster:

```
vserver services name-service dns show
                                         Name
Vserver      State     Domains           Servers
-----
cluster-1    enabled   xyz.company.com  192.56.0.129,
                                         192.56.0.130
vs1          enabled   xyz.company.com  192.56.0.129,
                                         192.56.0.130
vs2          enabled   xyz.company.com  192.56.0.129,
                                         192.56.0.130
vs3          enabled   xyz.company.com  192.56.0.129,
                                         192.56.0.130
```

The following command displays detailed DNS configuration information for SVM vs1:

```
vserver services name-service dns show -vserver vs1
    Vserver: vs1
        Domains: xyz.company.com
        Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
    Maximum Attempts: 1
```

Display information about failover groups

You can view information about failover groups, including the list of nodes and ports in each failover group, whether failover is enabled or disabled, and the type of failover policy that is being applied to each LIF.

Steps

1. Display the target ports for each failover group by using the [network interface failover-groups show](#) command.

The following command displays information about all failover groups on a two-node cluster:

```
network interface failover-groups show
    Failover
Vserver      Group      Targets
-----
Cluster
    Cluster
        cluster1-01:e0a, cluster1-01:e0b,
        cluster1-02:e0a, cluster1-02:e0b
vs1
    Default
        cluster1-01:e0c, cluster1-01:e0d,
        cluster1-01:e0e, cluster1-02:e0c,
        cluster1-02:e0d, cluster1-02:e0e
```

2. Display the target ports and broadcast domain for a specific failover group by using the [network interface failover-groups show](#) command.

The following command displays detailed information about failover group data12 for SVM vs4:

```

network interface failover-groups show -vserver vs4 -failover-group
data12

    Vserver Name: vs4
    Failover Group Name: data12
    Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                      cluster1-02:e0g
    Broadcast Domain: Default

```

3. Display the failover settings used by all LIFs by using the `network interface show` command.

The following command displays the failover policy and failover group that is being used by each LIF:

network interface show -vserver * -lif * -fields failover-group,failover-policy			
vserver	lif	failover-policy	failover-group
Cluster	cluster1-01_clus_1	local-only	Cluster
Cluster	cluster1-01_clus_2	local-only	Cluster
Cluster	cluster1-02_clus_1	local-only	Cluster
Cluster	cluster1-02_clus_2	local-only	Cluster
cluster1	cluster_mgmt	broadcast-domain-wide	Default
cluster1	cluster1-01_mgmt1	local-only	Default
cluster1	cluster1-02_mgmt1	local-only	Default
vs1	data1	disabled	Default
vs3	data2	system-defined	group2

Display LIF failover targets

You might have to check whether the failover policies and the failover groups of a LIF are configured correctly. To prevent misconfiguration of the failover rules, you can display the failover targets for a single LIF or for all LIFs.

About this task

Displaying LIF failover targets enables you to check for the following:

- Whether the LIFs are configured with the correct failover group and failover policy
- Whether the resulting list of failover target ports is appropriate for each LIF
- Whether the failover target of a data LIF is not a management port (e0M)

Step

Display the failover targets of a LIF by using the `failover` option of the `network interface show` command.

The following command displays information about the failover targets for all LIFs in a two-node cluster. The

Failover Targets row shows the (prioritized) list of node-port combinations for a given LIF.

network interface show -failover		Logical Interface	Home Node:Port	Failover Policy	Failover Group
Cluster					
node1_clus1	node1:e0a		local-only	Cluster	
		Failover Targets:	node1:e0a, node1:e0b		
node1_clus2	node1:e0b		local-only	Cluster	
		Failover Targets:	node1:e0b, node1:e0a		
node2_clus1	node2:e0a		local-only	Cluster	
		Failover Targets:	node2:e0a, node2:e0b		
node2_clus2	node2:e0b		local-only	Cluster	
		Failover Targets:	node2:e0b, node2:e0a		
cluster1					
cluster_mgmt	node1:e0c		broadcast-domain-wide		Default
		Failover Targets:	node1:e0c, node1:e0d, node2:e0c, node2:e0d		
node1_mgmt1	node1:e0c		local-only	Default	
		Failover Targets:	node1:e0c, node1:e0d		
node2_mgmt1	node2:e0c		local-only	Default	
		Failover Targets:	node2:e0c, node2:e0d		
vs1					
data1	node1:e0e		system-defined	bcast1	
		Failover Targets:	node1:e0e, node1:e0f, node2:e0e, node2:e0f		

Display LIFs in a load balancing zone

You can verify whether a load balancing zone is configured correctly by displaying all of the LIFs that belong to it. You can also view the load balancing zone of a particular LIF, or the load balancing zones for all LIFs.

Step

Display the LIFs and load balancing details that you want by using one of the following commands

To display...	Enter...
LIFs in a particular load balancing zone	network interface show -dns-zone zone_name zone_name specifies the name of the load balancing zone
The load balancing zone of a particular LIF	network interface show -lif lif_name -fields dns-zone
The load balancing zones of all LIFs	network interface show -fields dns-zone

Examples of displaying load balancing zones for LIFs

The following command displays the details of all LIFs in the load balancing zone storage.company.com for SVM vs0:

```
net int show -vserver vs0 -dns-zone storage.company.com

      Logical      Status      Network          Current      Current  Is
Vserver  Interface  Admin/Oper Address/Mask    Node        Port     Home
-----  -----  -----
vs0
      lif3       up/up    10.98.226.225/20  ndeux-11  e0c      true
      lif4       up/up    10.98.224.23/20   ndeux-21  e0c      true
      lif5       up/up    10.98.239.65/20  ndeux-11  e0c      true
      lif6       up/up    10.98.239.66/20  ndeux-11  e0c      true
      lif7       up/up    10.98.239.63/20  ndeux-21  e0c      true
      lif8       up/up    10.98.239.64/20  ndeux-21  e0c      true
```

The following command displays the DNS zone details of the LIF data3:

```
network interface show -lif data3 -fields dns-zone
Vserver  lif      dns-zone
-----  -----  -----
vs0      data3    storage.company.com
```

The following command displays the list of all LIFs in the cluster and their corresponding DNS zones:

```
network interface show -fields dns-zone
Vserver    lif          dns-zone
-----
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1       none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

Display cluster connections

You can display all the active connections in the cluster or a count of active connections on the node by client, logical interface, protocol, or service. You can also display all the listening connections in the cluster.

Display active connections by client (cluster administrators only)

You can view the active connections by client to verify the node that a specific client is using and to view possible imbalances between client counts per node.

About this task

The count of active connections by client is useful in the following scenarios:

- Finding a busy or overloaded node.
- Determining why a particular client's access to a volume is slow.

You can view details about the node that the client is accessing and then compare it with the node on which the volume resides. If accessing the volume requires traversing the cluster network, clients might experience decreased performance because of the remote access to the volume on an oversubscribed remote node.

- Verifying that all nodes are being used equally for data access.
- Finding clients that have an unexpectedly high number of connections.
- Verifying whether certain clients have connections to a node.

Step

Display a count of the active connections by client on a node by using the `network connections active show-clients` command.

For more information about this command, see the man page: [ONTAP 9 commands](#)

network connections active show-clients			
Node	Vserver Name	Client IP Address	Count
node0	vs0	192.0.2.253	1
	vs0	192.0.2.252	2
	Cluster	192.10.2.124	5
node1	vs0	192.0.2.250	1
	vs0	192.0.2.252	3
	Cluster	192.10.2.123	4
node2	vs1	customer.example.com	1
	vs1	192.0.2.245	3
	Cluster	192.10.2.122	4
node3	vs1	customer.example.org	1
	vs1	customer.example.net	3
	Cluster	192.10.2.121	4

Display active connections by protocol (cluster administrators only)

You can display a count of the active connections by protocol (TCP or UDP) on a node to compare the usage of protocols within the cluster.

About this task

The count of active connections by protocol is useful in the following scenarios:

- Finding the UDP clients that are losing their connection.

If a node is near its connection limit, UDP clients are the first to be dropped.

- Verifying that no other protocols are being used.

Step

Display a count of the active connections by protocol on a node by using the `network connections active show-protocols` command.

For more information about this command, see the man page.

network connections active show-protocols				
Node	Vserver	Name	Protocol	Count
node0		vs0	UDP	19
		Cluster	TCP	11
node1		vs0	UDP	17
		Cluster	TCP	8
node2		vs1	UDP	14
		Cluster	TCP	10
node3		vs1	UDP	18
		Cluster	TCP	4

Display active connections by service (cluster administrators only)

You can display a count of the active connections by service type (for example, by NFS, SMB, mount, and so on) for each node in a cluster. This is useful to compare the usage of services within the cluster, which helps to determine the primary workload of a node.

About this task

The count of active connections by service is useful in the following scenarios:

- Verifying that all nodes are being used for the appropriate services and that the load balancing for that service is working.
- Verifying that no other services are being used. Display a count of the active connections by service on a node by using the `network connections active show-services` command.

For more information about this command, see the man page: [ONTAP 9 commands](#)

network connections active show-services			
Node	Vserver Name	Service	Count
node0			
	vs0	mount	3
	vs0	nfs	14
	vs0	nlm_v4	4
	vs0	cifs_srv	3
	vs0	port_map	18
	vs0	rclopcp	27
	Cluster	ctlopcp	60
node1			
	vs0	cifs_srv	3
	vs0	rclopcp	16
	Cluster	ctlopcp	60
node2			
	vs1	rclopcp	13
	Cluster	ctlopcp	60
node3			
	vs1	cifs_srv	1
	vs1	rclopcp	17
	Cluster	ctlopcp	60

Display active connections by LIF on a node and SVM

You can display a count of active connections for each LIF, by node and storage virtual machine (SVM), to view connection imbalances between LIFs within the cluster.

About this task

The count of active connections by LIF is useful in the following scenarios:

- Finding an overloaded LIF by comparing the number of connections on each LIF.
- Verifying that DNS load balancing is working for all data LIFs.
- Comparing the number of connections to the various SVMs to find the SVMs that are used the most.

Step

Display a count of active connections for each LIF by SVM and node by using the `network connections active show-lifs` command.

For more information about this command, see the man page: [ONTAP 9 commands](#)

network connections active show-lifs			
Node	Vserver Name	Interface Name	Count
node0			
	vs0	dataif1	3
	Cluster	node0_clus_1	6
	Cluster	node0_clus_2	5
node1			
	vs0	dataif2	3
	Cluster	node1_clus_1	3
	Cluster	node1_clus_2	5
node2			
	vs1	dataif2	1
	Cluster	node2_clus_1	5
	Cluster	node2_clus_2	3
node3			
	vs1	dataif1	1
	Cluster	node3_clus_1	2
	Cluster	node3_clus_2	2

Display active connections in a cluster

You can display information about the active connections in a cluster to view the LIF, port, remote host, service, storage virtual machines (SVMs), and protocol used by individual connections.

About this task

Viewing the active connections in a cluster is useful in the following scenarios:

- Verifying that individual clients are using the correct protocol and service on the correct node.
- If a client is having trouble accessing data using a certain combination of node, protocol, and service, you can use this command to find a similar client for configuration or packet trace comparison.

Step

Display the active connections in a cluster by using the `network connections active show` command.

For more information about this command, see the man page: [ONTAP 9 commands](#)

The following command shows the active connections on the node node1:

```

network connections active show -node node1
Vserver  Interface          Remote
Name     Name:Local Port    Host:Port      Protocol/Service
-----
Node: node1
Cluster  node1_clus_1:50297 192.0.2.253:7700  TCP/ctlopcp
Cluster  node1_clus_1:13387 192.0.2.253:7700  TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700  TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700  TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700  TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map

```

The following command shows the active connections on SVM vs1:

```

network connections active show -vserver vs1
Vserver  Interface          Remote
Name     Name:Local Port    Host:Port      Protocol/Service
-----
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map

```

Display listening connections in a cluster

You can display information about the listening connections in a cluster to view the LIFs and ports that are accepting connections for a given protocol and service.

About this task

Viewing the listening connections in a cluster is useful in the following scenarios:

- Verifying that the desired protocol or service is listening on a LIF if client connections to that LIF fail consistently.
- Verifying that a UDP/ctlopcp listener is opened at each cluster LIF if remote data access to a volume on one node through a LIF on another node fails.
- Verifying that a UDP/ctlopcp listener is opened at each cluster LIF if SnapMirror transfers between two nodes in the same cluster fail.
- Verifying that a TCP/ctlopcp listener is opened at each intercluster LIF if SnapMirror transfers between two nodes in different clusters fail.

Step

Display the listening connections per node by using the `network connections listening show` command.

network connections listening show		
Vserver Name	Interface Name:Local Port	Protocol/Service
Node: node0		
Cluster	node0_clus_1:7700	TCP/ctlopcp
vs1	data1:4049	UDP/unknown
vs1	data1:111	TCP/port-map
vs1	data1:111	UDP/port-map
vs1	data1:4046	TCP/sm
vs1	data1:4046	UDP/sm
vs1	data1:4045	TCP/nlm-v4
vs1	data1:4045	UDP/nlm-v4
vs1	data1:2049	TCP/nfs
vs1	data1:2049	UDP/nfs
vs1	data1:635	TCP/mount
vs1	data1:635	UDP/mount
Cluster	node0_clus_2:7700	TCP/ctlopcp

Commands for diagnosing network problems

You can diagnose problems on your network by using commands such as [ping](#), [traceroute](#), [ndp](#), and [tcpdump](#). You can also use commands such as [ping6](#) and [traceroute6](#) to diagnose IPv6 problems.

If you want to...	Enter this command...
Test whether the node can reach other hosts on your network	network ping
Test whether the node can reach other hosts on your IPv6 network	network ping6
Trace the route that the IPv4 packets take to a network node	network traceroute
Trace the route that the IPv6 packets take to a network node	network traceroute6
Manage the Neighbor Discovery Protocol (NDP)	network ndp
Display statistics about packets that are received and sent on a specified network interface or on all network interfaces	run -node node_name ifstat Note: This command is available from the nodeshell.
Display information about neighboring devices that are discovered from each node and port in the cluster, including the remote device type and device platform	network device-discovery show
View the CDP neighbors of the node (ONTAP supports only CDPv1 advertisements)	run -node node_name cdpd show-neighbors Note: This command is available from the nodeshell.

If you want to...	Enter this command...
Trace the packets that are sent and received in the network	network tcpdump start -node node-name - port port_name Note: This command is available from the nodeshell.
Measure latency and throughput between intercluster or intracluster nodes	network test-path -source-node source_nodename
local -destination- cluster destination_clustername - destination-node destination_nodename - session-type Default	AsyncMirrorLocal
AsyncMirrorRemote	SyncMirrorRemote

For more information about these commands, see the appropriate man pages: [ONTAP 9 commands](#)

Display network connectivity with neighbor discovery protocols

In a data center, you can use neighbor discovery protocols to view network connectivity between a pair of physical or virtual systems and their network interfaces. ONTAP supports two neighbor discovery protocols: Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).

About this task

Neighbor discovery protocols enable you to automatically discover and view information about directly connected protocol-enabled devices in a network. Each device advertises identification, capabilities, and connectivity information. This information is transmitted in Ethernet frames to a multicast MAC address and is received by all neighboring protocol-enabled devices.

For two devices to become neighbors, each must have a protocol enabled and correctly configured. Discovery protocol functionality is limited to directly connected networks. Neighbors can include protocol-enabled devices such as switches, routers, bridges, and so on. ONTAP supports two neighbor discovery protocols, which can be used individually or together.

Cisco Discovery Protocol (CDP)

CDP is a proprietary link layer protocol developed by Cisco Systems. It is enabled by default in ONTAP for cluster ports, but must be enabled explicitly for data ports.

Link Layer Discovery Protocol (LLDP)

LLDP is a vendor-neutral protocol specified in the standards document IEEE 802.1AB. It must be enabled explicitly for all ports.

Use CDP to detect network connectivity

Using CDP to detect network connectivity consists of reviewing deployment considerations, enabling it on data ports, viewing neighbor devices, and adjusting CDP configuration values as needed. CDP is enabled by default on cluster ports.

CDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

CDP is also used by the cluster switch health monitor to automatically discover your cluster and management

network switches.

Related information

[System administration](#)

Considerations for using CDP

By default, CDP-compliant devices send CDPv2 advertisements. CDP-compliant devices send CDPv1 advertisements only when they receive CDPv1 advertisements. ONTAP supports only CDPv1. Therefore, when an ONTAP node sends CDPv1 advertisements, CDP-compliant neighboring devices send back CDPv1 advertisements.

You should consider the following information before enabling CDP on a node:

- CDP is always enabled on cluster ports.
- CDP is disabled, by default, on all non-cluster ports.
- CDP is supported for all ports.
- CDP advertisements are sent and received by ports that are in the up state.
- CDP must be enabled on both the transmitting and receiving devices for sending and receiving CDP advertisements.
- CDP advertisements are sent at regular intervals, and you can configure the time interval.
- When IP addresses are changed for a LIF, the node sends the updated information in the next CDP advertisement.



Sometimes when LIFs are changed on the node, the CDP information is not updated at the receiving device side (for example, a switch). If you encounter such a problem, you should configure the network interface of the node to the down status and then to the up status.

- Only IPv4 addresses are advertised in CDP advertisements.
- For physical network ports with VLANs, all of the LIFs configured on the VLANs on that port are advertised.
- For physical ports that are part of an interface group, all of the IP addresses configured on that interface group are advertised on each physical port.
- For an interface group that hosts VLANs, all of the LIFs configured on the interface group and the VLANs are advertised on each of the network ports.
- For packets with MTU size equal to or greater than 1,500 bytes, only the number of LIFs that can fit into a 1500 MTU-sized packet is advertised.

Enable or disable CDP

To discover and send advertisements to CDP-compliant neighboring devices, CDP must be enabled on each node of the cluster. By default, CDP is enabled on all cluster ports of a node and disabled on all non-cluster ports of a node.

About this task

The `cdpd.enable` option controls whether CDP is enabled or disabled on the ports of a node:

- `on` enables CDP on non-cluster ports.
- `off` disables CDP on non-cluster ports; you cannot disable CDP on cluster ports.

When CDP is disabled on a port that is connected to a CDP-compliant device, network traffic might not be optimized.

Steps

1. Display the current CDP setting for a node, or for all nodes in a cluster:

To view the CDP setting of...	Enter
A node	run - node <node_name> options cdpd.enabled
All nodes in a cluster	options cdpd.enabled

2. Enable or disable CDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable CDP on...	Enter...
A node	run -node node_name options cdpd.enable {on or off}
All nodes in a cluster	options cdpd.enable {on or off}

View CDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to a CDP-compliant device. You can use the `network device-discovery show -protocol cdp` command to view neighbor information.

About this task

Because CDP is always enabled for cluster ports, CDP neighbor information is always displayed for those ports. CDP must be enabled on non-cluster ports for neighbor information to appear for those ports.

Step

Display information about all CDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol cdp
```

The following command shows the neighbors that are connected to the ports on node cluster-1_01:

```

network device-discovery show -node sti2650-212 -protocol cdp
Node/      Local   Discovered
Protocol    Port    Device (LLDP: ChassisID)  Interface          Platform
-----
-----
sti2650-212/cdp
    e0M      RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                           Ethernet1/14          N9K-
C93120TX
    e0a      CS:RTP-CS01-510K35        0/8            CN1610
    e0b      CS:RTP-CS01-510K36        0/8            CN1610
    e0c      RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                           Ethernet1/21          N9K-
C93180YC-FX
    e0d      RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                           Ethernet1/22          N9K-
C93180YC-FX
    e0e      RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                           Ethernet1/23          N9K-
C93180YC-FX
    e0f      RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                           Ethernet1/24          N9K-
C93180YC-FX

```

The output lists the Cisco devices that are connected to each port of the specified node.

Configure the hold time for CDP messages

Hold time is the period of time for which CDP advertisements are stored in cache in neighboring CDP-compliant devices. Hold time is advertised in each CDPv1 packet and is updated whenever a CDPv1 packet is received by a node.

- The value of the `cdpd.holdtime` option should be set to the same value on both nodes of an HA pair.
- The default hold time value is 180 seconds, but you can enter values ranging from 10 seconds to 255 seconds.
- If an IP address is removed before the hold time expires, the CDP information is cached until the hold time expires.

Steps

1. Display the current CDP hold time for a node, or for all nodes in a cluster:

To view the hold time of...	Enter...
A node	<code>run -node node_name options cdpd.holdtime</code>
All nodes in a cluster	<code>options cdpd.holdtime</code>

2. Configure the CDP hold time on all ports of a node, or on all ports of all nodes in a cluster:

To set the hold time on...	Enter...
A node	<code>run -node node_name options cdpd.holdtime holdtime</code>
All nodes in a cluster	<code>options cdpd.holdtime holdtime`</code>

Set the interval for sending CDP advertisements

CDP advertisements are sent to CDP neighbors at periodic intervals. You can increase or decrease the interval for sending CDP advertisements depending on network traffic and changes in the network topology.

- The value of the `cdpd.interval` option should be set to the same value on both nodes of an HA pair.
- The default interval is 60 seconds, but you can enter a value from 5 seconds to 900 seconds.

Steps

1. Display the current CDP advertisement time interval for a node, or for all nodes in a cluster:

To view the interval for...	Enter...
A node	<code>run -node node_name options cdpd.interval</code>
All nodes in a cluster	<code>options cdpd.interval</code>

2. Configure the interval for sending CDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

To set the interval for...	Enter...
A node	<code>run -node node_name options cdpd.interval interval</code>
All nodes in a cluster	<code>options cdpd.interval interval</code>

View or clear CDP statistics

You can view the CDP statistics for the cluster and non-cluster ports on each node to detect potential network connectivity issues. CDP statistics are cumulative from the time they were last cleared.

About this task

Because CDP is always enabled for cluster ports, CDP statistics are always displayed for traffic on those ports. CDP must be enabled on non-cluster ports for statistics to appear for those ports.

Step

Display or clear the current CDP statistics for all ports on a node:

If you want to...	Enter...
View the CDP statistics	<code>run -node node_name cdpd show-stats</code>

If you want to...	Enter...
Clear the CDP statistics	run -node node_name cdpd zero-stats

Example of showing and clearing statistics

The following command shows the CDP statistics before they are cleared. The output displays the total number of packets that have been sent and received since the last time the statistics were cleared.

```
run -node node1 cdpd show-stats

RECEIVE
  Packets:      9116 | Csum Errors:      0 | Unsupported Vers:  4561
  Invalid length: 0 | Malformed:      0 | Mem alloc fails:  0
  Missing TLVs:   0 | Cache overflow:  0 | Other errors:    0

TRANSMIT
  Packets:      4557 | Xmit fails:      0 | No hostname:    0
  Packet truncated: 0 | Mem alloc fails:  0 | Other errors:    0

OTHER
  Init failures: 0
```

The following command clears the CDP statistics:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
  Packets:      0 | Csum Errors:      0 | Unsupported Vers:  0
  Invalid length: 0 | Malformed:      0 | Mem alloc fails:  0
  Missing TLVs:   0 | Cache overflow:  0 | Other errors:    0

TRANSMIT
  Packets:      0 | Xmit fails:      0 | No hostname:    0
  Packet truncated: 0 | Mem alloc fails:  0 | Other errors:    0

OTHER
  Init failures: 0
```

After the statistics are cleared, they begin to accumulate after the next CDP advertisement is sent or received.

Use LLDP to detect network connectivity

Using LLDP to detect network connectivity consists of reviewing deployment considerations, enabling it on all ports, viewing neighbor devices, and adjusting LLDP configuration values as needed.

LLDP must also be enabled on any switches and routers before information about neighbor devices can be displayed.

ONTAP currently reports the following type-length-value structures (TLVs):

- Chassis ID
- Port ID
- Time-To-Live (TTL)
- System name

The system name TLV is not sent on CNA devices.

Certain converged network adapters (CNAs), such as the X1143 adapter and the UTA2 onboard ports, contain offload support for LLDP:

- LLDP offload is used for Data Center Bridging (DCB).
- Displayed information might differ between the cluster and the switch.

For example, the Chassis ID and Port ID data displayed by the switch might be different for CNA and non-CNA ports, but the data displayed by the cluster is consistent for these port types.



The LLDP specification defines access to the collected information through an SNMP MIB. However, ONTAP does not currently support the LLDP MIB.

Enable or disable LLDP

To discover and send advertisements to LLDP-compliant neighboring devices, LLDP must be enabled on each node of the cluster. Starting with ONTAP 9.7, LLDP is enabled on all ports of a node by default.

About this task

The `lldp.enable` option controls whether LLDP is enabled or disabled on the ports of a node:

- `on` enables LLDP on all ports.
- `off` disables LLDP on all ports.

Steps

1. Display the current LLDP setting for a node, or for all nodes in a cluster:

- Single node: `run -node node_name options lldp.enable`
- All nodes: `options lldp.enable`

2. Enable or disable LLDP on all ports of a node, or on all ports of all nodes in a cluster:

To enable or disable LLDP on...	Enter...
A node	run -node node_name options lldp.enable {on off}
All nodes in a cluster	options lldp.enable {on off}

- Single node:

```
run -node node_name options lldp.enable {on|off}
```

- All nodes:

```
options lldp.enable {on|off}
```

View LLDP neighbor information

You can view information about the neighboring devices that are connected to each port of the nodes of your cluster, provided that the port is connected to an LLDP-compliant device. You use the network device-discovery show command to view neighbor information.

Step

Display information about all LLDP-compliant devices that are connected to the ports on a node in the cluster:

```
network device-discovery show -node node -protocol lldp
```

The following command shows the neighbors that are connected to the ports on node cluster-1_01. The output lists the LLDP-enabled devices that are connected to each port of the specified node. If the `-protocol` option is omitted, the output also lists CDP-enabled devices.

network device-discovery show -node cluster-1_01 -protocol lldp				
Node/Protocol	Local Port	Discovered Device	Interface	Platform
cluster-1_01/lldp	e2a	0013.c31e.5c60	GigabitEthernet1/36	
	e2b	0013.c31e.5c60	GigabitEthernet1/35	
	e2c	0013.c31e.5c60	GigabitEthernet1/34	
	e2d	0013.c31e.5c60	GigabitEthernet1/33	

Adjust the interval for transmitting LLDP advertisements

LLDP advertisements are sent to LLDP neighbors at periodic intervals. You can increase or decrease the interval for sending LLDP advertisements depending on network traffic and changes in the network topology.

About this task

The default interval recommended by IEEE is 30 seconds, but you can enter a value from 5 seconds to 300 seconds.

Steps

1. Display the current LLDP advertisement time interval for a node, or for all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.interval
```

- All nodes:

```
options lldp.xmit.interval
```

2. Adjust the interval for sending LLDP advertisements for all ports of a node, or for all ports of all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.interval <interval>
```

- All nodes:

```
options lldp.xmit.interval <interval>
```

Adjust the time-to-live value for LLDP advertisements

Time-To-Live (TTL) is the period of time for which LLDP advertisements are stored in cache in neighboring LLDP-compliant devices. TTL is advertised in each LLDP packet and is updated whenever an LLDP packet is received by a node. TTL can be modified in outgoing LLDP frames.

About this task

- TTL is a calculated value, the product of the transmit interval (`lldp.xmit.interval`) and the hold multiplier (`lldp.xmit.hold`) plus one.
- The default hold multiplier value is 4, but you can enter values ranging from 1 to 100.
- The default TTL is therefore 121 seconds, as recommended by IEEE, but by adjusting the transmit interval and hold multiplier values, you can specify a value for outgoing frames from 6 seconds to 30001 seconds.
- If an IP address is removed before the TTL expires, the LLDP information is cached until the TTL expires.

Steps

1. Display the current hold multiplier value for a node, or for all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.hold
```

- All nodes:

```
options lldp.xmit.hold
```

2. Adjust the hold multiplier value on all ports of a node, or on all ports of all nodes in a cluster:

- Single node:

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

- All nodes:

```
options lldp.xmit.hold <hold_value>
```

Get more information

You can get help and find more information through various resources, documentation, and forums.

- [Documentation](#) – Release Notes and Guides for this release and previous releases.
- [NetApp TechCommTV](#) – NetApp videos.
- [NetApp resources](#) – Technical Reports and Knowledgebase Articles.
- [NetApp Community](#) – NetApp product and solutions forums.

High Availability

Cluster nodes are configured in high-availability (HA) pairs for fault tolerance and nondisruptive operations. If a node fails or if you need to bring a node down for routine maintenance, its partner can take over its storage and continue to serve data from it. The partner gives back storage when the node is brought back on line.

The HA pair controller configuration consists of a pair of matching FAS/AFF storage controllers (local node and partner node). Each of these nodes is connected to the other's disk shelves. When one node in an HA pair encounters an error and stops processing data, its partner detects the failed status of the partner and takes over all data processing from that controller.

Takeover is the process in which a node assumes control of its partner's storage.

Giveback is the process in which the storage is returned to the partner.

By default, takeovers occur automatically in any of the following situations:

- A software or system failure occurs on a node that leads to a panic. The HA pair controllers automatically fail over to their partner node. After the partner has recovered from the panic and booted up, the node automatically performs a giveback, returning the partner to normal operation.
- A system failure occurs on a node, and the node cannot reboot. For example, when a node fails because of a power loss, HA pair controllers automatically fail over to their partner node and serve data from the surviving storage controller.



If the storage for a node also loses power at the same time, a standard takeover is not possible.

- Heartbeat messages are not received from the node's partner. This could happen if the partner experienced a hardware or software failure (for example, an interconnect failure) that did not result in a panic but still prevented it from functioning correctly.
- You halt one of the nodes without using the `-f` or `-inhibit-takeover true` parameter.



In a two-node cluster with cluster HA enabled, halting or rebooting a node using the `-inhibit-takeover true` parameter causes both nodes to stop serving data unless you first disable cluster HA and then assign epsilon to the node that you want to remain online.

- You reboot one of the nodes without using the `-inhibit-takeover true` parameter. (The `-onboot` parameter of the `storage failover` command is enabled by default.)
- The remote management device (Service Processor) detects failure of the partner node. This is not applicable if you disable hardware-assisted takeover.

You can also manually initiate takeovers with the `storage failover takeover` command.

How hardware-assisted takeover works

Enabled by default, the hardware-assisted takeover feature can speed up the takeover process by using a node's remote management device (Service Processor).

When the remote management device detects a failure, it quickly initiates the takeover rather than waiting for ONTAP to recognize that the partner's heartbeat has stopped. If a failure occurs without this feature enabled, the partner waits until it notices that the node is no longer giving a heartbeat, confirms the loss of heartbeat, and then initiates the takeover.

The hardware-assisted takeover feature uses the following process to avoid that wait:

1. The remote management device monitors the local system for certain types of failures.
2. If a failure is detected, the remote management device immediately sends an alert to the partner node.
3. Upon receiving the alert, the partner initiates takeover.

System events that trigger hardware-assisted takeover

The partner node might generate a takeover depending on the type of alert it receives from the remote management device (Service Processor).

Alert	Takeover initiated upon receipt?	Description
abnormal_reboot	No	An abnormal reboot of the node occurred.
l2_watchdog_reset	Yes	The system watchdog hardware detected an L2 reset. The remote management device detected a lack of response from the system CPU and reset the system.
loss_of_heartbeat	No	The remote management device is no longer receiving the heartbeat message from the node. This alert does not refer to the heartbeat messages between the nodes in the HA pair; it refers to the heartbeat between the node and its local remote management device.
periodic_message	No	A periodic message is sent during a normal hardware-assisted takeover operation.
power_cycle_via_sp	Yes	The remote management device cycled the system power off and on.
power_loss	Yes	A power loss occurred on the node. The remote management device has a power supply that maintains power for a short period after a power loss, allowing it to report the power loss to the partner.
power_off_via_sp	Yes	The remote management device powered off the system.

Alert	Takeover initiated upon receipt?	Description
reset_via_sp	Yes	The remote management device reset the system.
test	No	A test message is sent to verify a hardware-assisted takeover operation.

How automatic takeover and giveback works

The automatic takeover and giveback operations can work together to reduce and avoid client outages.

By default, if one node in the HA pair panics, reboots, or halts, the partner node automatically takes over and then returns storage when the affected node reboots. The HA pair then resumes a normal operating state.

Automatic takeovers may also occur if one of the nodes become unresponsive.

Automatic giveback occurs by default. If you would rather control giveback impact on clients, you can disable automatic giveback and use the `storage failover modify -auto-giveback false -node <node>` command. Before performing the automatic giveback (regardless of what triggered it), the partner node waits for a fixed amount of time as controlled by the `-delay- seconds` parameter of the `storage failover modify` command. The default delay is 600 seconds. By delaying the giveback, the process results in two brief outages: one during takeover and one during giveback.

This process avoids a single, prolonged outage that includes time required for:

- The takeover operation
- The taken-over node to boot up to the point at which it is ready for the giveback
- The giveback operation

If the automatic giveback fails for any of the non-root aggregates, the system automatically makes two additional attempts to complete the giveback.



During the takeover process, the automatic giveback process starts before the partner node is ready for the giveback. When the time limit of the automatic giveback process expires and the partner node is still not ready, the timer restarts. As a result, the time between the partner node being ready and the actual giveback being performed might be shorter than the automatic giveback time.

What happens during takeover

When a node takes over its partner, it continues to serve and update data in the partner's aggregates and volumes.

The following steps occur during the takeover process:

1. If the negotiated takeover is user-initiated, aggregated data is moved from the partner node to the node that is performing the takeover. A brief outage occurs as the current owner of each aggregate (except for the root aggregate) changes over to the takeover node. This outage is briefer than an outage that occurs during a takeover without aggregate relocation.

- You can monitor the progress using the `storage failover show-takeover` command.
- You can avoid the aggregate relocation during this takeover instance by using the `-bypass-optimization` parameter with the `storage failover takeover` command.



Aggregates are relocated serially during planned takeover operations to reduce client outage. If aggregate relocation is bypassed, longer client outage occurs during planned takeover events.

2. If the user-initiated takeover is a negotiated takeover, the target node gracefully shuts down, followed by takeover of the target node's root aggregate and any aggregates that were not relocated in Step 1.
3. Before the storage takeover begins, data LIFs (logical interfaces) migrate from the target node to the takeover node, or to any other node in the cluster based on LIF failover rules. You can avoid the LIF migration by using the `-skip-lif-migration` parameter with the `storage failover takeover` command.
4. Existing SMB (CIFS) sessions are disconnected when takeover occurs.



Due to the nature of the SMB protocol, all SMB sessions are disrupted (except for SMB 3.0 sessions connected to shares with the Continuous Availability property set). SMB 1.0 and SMB 2.x sessions cannot reconnect after a takeover event; therefore, takeover is disruptive and some data loss could occur.

5. SMB 3.0 sessions that are established to shares with the Continuous Availability property enabled can reconnect to the disconnected shares after a takeover event. If your site uses SMB 3.0 connections to Microsoft Hyper-V and the Continuous Availability property is enabled on the associated shares, takeovers are non-disruptive for those sessions.

What happens if a node performing a takeover panics

If the node that is performing the takeover panics within 60 seconds of initiating takeover, the following events occur:

- The node that panicked reboots.
- After it reboots, the node performs self-recovery operations and is no longer in takeover mode.
- Failover is disabled.
- If the node still owns some of the partner's aggregates, after enabling storage failover, return these aggregates to the partner using the `storage failover giveback` command.

What happens during giveback

The local node returns ownership to the partner node when issues are resolved, when the partner node boots up, or when giveback is initiated.

The following process takes place in a normal giveback operation. In this discussion, Node A has taken over Node B. Any issues on Node B have been resolved and it is ready to resume serving data.

1. Any issues on Node B are resolved and it displays the following message: `Waiting for giveback`
2. The giveback is initiated by the `storage failover giveback` command or by automatic giveback if the system is configured for it. This initiates the process of returning ownership of Node B's aggregates and volumes from Node A back to Node B.

3. Node A returns control of the root aggregate first.
4. Node B completes the process of booting up to its normal operating state.
5. As soon as Node B reaches the point in the boot process where it can accept the non-root aggregates, Node A returns ownership of the other aggregates, one at a time, until giveback is complete. You can monitor the progress of the giveback by using the `storage failover show-giveback` command.



The `storage failover show-giveback` command does not (nor is it intended to) display information about all operations occurring during the storage failover giveback operation. You can use the `storage failover show` command to display additional details about the current failover status of the node, such as if the node is fully functional, takeover is possible, and giveback is complete.

I/O resumes for each aggregate after giveback is complete for that aggregate, which reduces its overall outage window.

HA policy and its effect on takeover and giveback

ONTAP automatically assigns an HA policy of CFO (controller failover) and SFO (storage failover) to an aggregate. This policy determines how storage failover operations occur for the aggregate and its volumes.

The two options, CFO and SFO, determine the aggregate control sequence ONTAP uses during storage failover and giveback operations.

Although the terms CFO and SFO are sometimes used informally to refer to storage failover (takeover and giveback) operations, they actually represent the HA policy assigned to the aggregates. For example, the terms SFO aggregate or CFO aggregate simply refer to the aggregate's HA policy assignment.

HA policies affect takeover and giveback operations as follows:

- Aggregates created on ONTAP systems (except for the root aggregate containing the root volume) have an HA policy of SFO. Manually initiated takeover is optimized for performance by relocating SFO (non-root) aggregates serially to the partner before takeover. During the giveback process, aggregates are given back serially after the taken-over system boots and the management applications come online, enabling the node to receive its aggregates.
- Because aggregate relocation operations entail reassigning aggregate disk ownership and shifting control from a node to its partner, only aggregates with an HA policy of SFO are eligible for aggregate relocation.
- The root aggregate always has an HA policy of CFO and is given back at the start of the giveback operation. This is necessary to allow the taken-over system to boot. All other aggregates are given back serially after the taken-over system completes the boot process and the management applications come online, enabling the node to receive its aggregates.



Changing the HA policy of an aggregate from SFO to CFO is a Maintenance mode operation. Do not modify this setting unless directed to do so by a customer support representative.

How background updates affect takeover and giveback

Background updates of the disk firmware will affect HA pair takeover, giveback, and aggregate relocation operations differently, depending on how those operations are initiated.

The following list describes how background disk firmware updates affect takeover, giveback, and aggregate

relocation:

- If a background disk firmware update occurs on a disk on either node, manually initiated takeover operations are delayed until the disk firmware update finishes on that disk. If the background disk firmware update takes longer than 120 seconds, takeover operations are aborted and must be restarted manually after the disk firmware update finishes. If the takeover was initiated with the `-bypass-optimization` parameter of the `storage failover takeover` command set to `true`, the background disk firmware update occurring on the destination node does not affect the takeover.
- If a background disk firmware update is occurring on a disk on the source (or takeover) node and the takeover was initiated manually with the `-options` parameter of the `storage failover takeover` command set to `immediate`, takeover operations start immediately.
- If a background disk firmware update is occurring on a disk on a node and it panics, takeover of the panicked node begins immediately.
- If a background disk firmware update is occurring on a disk on either node, giveback of data aggregates is delayed until the disk firmware update finishes on that disk.
- If the background disk firmware update takes longer than 120 seconds, giveback operations are aborted and must be restarted manually after the disk firmware update completes.
- If a background disk firmware update is occurring on a disk on either node, aggregate relocation operations are delayed until the disk firmware update finishes on that disk. If the background disk firmware update takes longer than 120 seconds, aggregate relocation operations are aborted and must be restarted manually after the disk firmware update finishes. If aggregate relocation was initiated with the `-override-destination-checks` of the `storage aggregate relocation` command set to `true`, the background disk firmware update occurring on the destination node does not affect aggregate relocation.

Automatic takeover commands

Automatic takeover is enabled by default on all supported NetApp FAS, AFF, and ASA platforms. You might need to change the default behavior and control when automatic takeovers occur when the partner node reboots, panics, or halts.

If you want takeover to occur automatically when the partner node...	Use this command...
Reboots or halts	<code>storage failover modify -node nodename -onreboot true</code>
Panics	<code>storage failover modify -node nodename -onpanic true</code>

Enable email notification if the takeover capability is disabled

To receive prompt notification if the takeover capability becomes disabled, you should configure your system to enable automatic email notification for the `takeover impossible` EMS messages:

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`

- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

Automatic giveback commands

In certain situations, you might need to manage your automatic giveback settings using ONTAP commands.

If you want to...	Use this command...
<p>Enable automatic giveback so that giveback occurs as soon as the taken-over node boots, reaches the Waiting for Giveback state, and the Delay before Auto Giveback period has expired.</p> <p>The default setting is true.</p>	<code>storage failover modify -node <i>nodename</i> -auto-giveback true</code>
<p>Disable automatic giveback. The default setting is true.</p> <p>Note: Setting this parameter to false does not disable automatic giveback after takeover on panic and takeover on reboot; automatic giveback after takeover on panic must be disabled by setting the <code>-auto-giveback-after-panic</code> parameter to false.</p>	<code>storage failover modify -node <i>nodename</i> -auto-giveback false</code>
<p>Disable automatic giveback after takeover on panic (this setting is enabled by default).</p>	<code>storage failover modify -node <i>nodename</i> -auto-giveback-after-panic false</code>
<p>Delay automatic giveback for a specified number of seconds (default is 600). This option determines the minimum time that a node remains in takeover before performing an automatic giveback.</p>	<code>storage failover modify -node <i>nodename</i> -delay-seconds <i>seconds</i></code>

How variations of the storage failover modify command affect automatic giveback

The operation of automatic giveback depends on how you configure the parameters of the storage failover modify command.

The following table lists the storage failover modify command parameters that apply to takeover events not caused by a panic:

Parameter	Default setting
-auto-giveback <i>true false</i>	<i>true</i>
-delay-seconds <i>integer (seconds)</i>	600
-onreboot <i>true false</i>	<i>true</i>

The following table describes how combinations of the `-onreboot` and `-auto-giveback` parameters affect automatic giveback for takeover events not caused by a panic.

storage failover modify parameters used	Cause of takeover	Does automatic giveback occur?
-onreboot <i>true</i>	reboot command	Yes
-auto-giveback <i>true</i>		
	halt command, or power cycle operation issued from the Service Processor	Yes
-onreboot <i>true</i>	reboot command	Yes
-auto-giveback <i>false</i>		
	halt command, or power cycle operation issued from the Service Processor	No
-onreboot <i>false</i>	reboot command	No
-auto-giveback <i>true</i>		
	halt command, or power cycle operation issued from the Service Processor	Yes
-onreboot <i>false</i>	reboot command	No
-auto-giveback <i>false</i>		
	halt command, or power cycle operation issued from the Service Processor	No



If the `-onreboot` parameter is set to true and a takeover occurs due to a reboot, then automatic giveback is always performed, regardless of whether the `-auto-giveback` parameter is set to true.

When the `-onreboot` parameter is set to false, a takeover does not occur in the case of a node reboot. Therefore, automatic giveback cannot occur, regardless of whether the `-auto-giveback` parameter is set to

true. A client disruption occurs.

The effects of automatic giveback parameter combinations that apply to panic situations.

The following table lists the `storage failover modify` command parameters that apply to panic situations:

Parameter	Default setting
<code>-onpanic true false</code>	<code>true</code>
<code>-auto-giveback-after-panic true false</code> (Privilege: Advanced)	<code>true</code>
<code>-auto-giveback true false</code>	<code>true</code>

The following table describes how parameter combinations of the `storage failover modify` command affect automatic giveback in panic situations.

storage failover parameters used	Does automatic giveback occur after panic?
<code>-onpanic false</code> <code>-auto-giveback-after-panic true</code>	No
<code>-onpanic false</code> <code>-auto-giveback-after-panic false</code>	No
<code>-onpanic true</code> <code>-auto-giveback true</code> <code>-auto-giveback-after-panic true</code>	Yes
<code>-onpanic true</code> <code>-auto-giveback true</code> <code>-auto-giveback-after-panic false</code>	No
<code>-onpanic true</code> <code>-auto-giveback false</code> <code>-auto-giveback-after-panic true</code>	Yes
<code>-onpanic true</code> <code>-auto-giveback false</code> <code>-auto-giveback-after-panic false</code>	No
<code>-onpanic false</code> If <code>-onpanic</code> is set to <code>false</code> , takeover/giveback does not occur, regardless of the value set for <code>-auto-giveback</code> or <code>-auto-giveback-after-panic</code>	No



If the `-onpanic` parameter is set to `true`, automatic giveback is always performed if a panic occurs unless you have changed the default settings for the `-auto-giveback` and `-auto-giveback-after-panic` parameters. If both of these parameters are changed from their default (`true`) to `false`, then an automatic giveback will not occur after a panic, even if the `-onpanic` parameter is set to `true`.

If the `-onpanic` parameter is set to `false`, takeover does not occur. Therefore, automatic giveback cannot occur, even if the auto giveback after panic parameter is set to `true`. A client disruption occurs.

Commands for monitoring an HA pair

You can use ONTAP commands to monitor the status of the HA pair. If a takeover occurs, you can also determine what caused the takeover.

If you want to check	Use this command
Whether failover is enabled or has occurred, or reasons why failover is not currently possible	<code>storage failover show</code>
View the nodes on which the storage failover HA-mode setting is enabled You must set the value to ha for the node to participate in a storage failover (HA pair) configuration. The <code>non-ha</code> value is used only in a stand-alone, or single node cluster configuration.	<code>storage failover show -fields mode</code>
Whether hardware-assisted takeover is enabled	<code>storage failover hwassist show</code>
The history of hardware-assisted takeover events that have occurred	<code>storage failover hwassist stats show</code>
The progress of a takeover operation as the partner's aggregates are moved to the node doing the takeover	<code>storage failover show-takeover</code>
The progress of a giveback operation in returning aggregates to the partner node	<code>storage failover show-giveback</code>
Whether an aggregate is home during takeover or giveback operations	<code>aggregate show -fields home-id,owner-id,home-name,owner-name,is-home</code>
Whether cluster HA is enabled (applies only to two node clusters)	<code>cluster ha show</code>
The HA state of the components of an HA pair (on systems that use the HA state)	<code>ha-config show</code> This is a Maintenance mode command.

Node states displayed by storage failover show-type commands

The following list describes the node states that the `storage failover show` command displays.

Node State	Description
Connected to partner_name, Automatic takeover disabled.	The HA interconnect is active and can transmit data to the partner node. Automatic takeover of the partner is disabled.
Waiting for partner_name, Giveback of partner spare disks pending.	<p>The local node cannot exchange information with the partner node over the HA interconnect. Giveback of SFO aggregates to the partner is done, but partner spare disks are still owned by the local node.</p> <ul style="list-style-type: none"> Run the <code>storage failover show-giveback</code> command for more information.
Waiting for partner_name. Waiting for partner lock synchronization.	The local node cannot exchange information with the partner node over the HA interconnect, and is waiting for partner lock synchronization to occur.
Waiting for partner_name. Waiting for cluster applications to come online on the local node.	The local node cannot exchange information with the partner node over the HA interconnect, and is waiting for cluster applications to come online.
Takeover scheduled. target node relocating its SFO aggregates in preparation of takeover.	Takeover processing has started. The target node is relocating ownership of its SFO aggregates in preparation for takeover.
Takeover scheduled. target node has relocated its SFO aggregates in preparation of takeover.	Takeover processing has started. The target node has relocated ownership of its SFO aggregates in preparation for takeover.
Takeover scheduled. Waiting to disable background disk firmware updates on local node. A firmware update is in progress on the node.	Takeover processing has started. The system is waiting for background disk firmware update operations on the local node to complete.
Relocating SFO aggregates to taking over node in preparation of takeover.	The local node is relocating ownership of its SFO aggregates to the taking-over node in preparation for takeover.
Relocated SFO aggregates to taking over node. Waiting for taking over node to takeover.	Relocation of ownership of SFO aggregates from the local node to the taking-over node has completed. The system is waiting for takeover by the taking-over node.
Relocating SFO aggregates to partner_name. Waiting to disable background disk firmware updates on the local node. A firmware update is in progress on the node.	Relocation of ownership of SFO aggregates from the local node to the taking-over node is in progress. The system is waiting for background disk firmware update operations on the local node to complete.

Node State	Description
Relocating SFO aggregates to partner_name. Waiting to disable background disk firmware updates on partner_name. A firmware update is in progress on the node.	Relocation of ownership of SFO aggregates from the local node to the taking-over node is in progress. The system is waiting for background disk firmware update operations on the partner node to complete.
Connected to partner_name. Previous takeover attempt was aborted because reason. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the "-bypass-optimization" parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because of the reason displayed under reason. The local node owns some of its partner's SFO aggregates. <ul style="list-style-type: none">• Either reissue a takeover of the partner node, setting the -bypass-optimization parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.
Connected to partner_name. Previous takeover attempt was aborted. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the "-bypass-optimization" parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted. The local node owns some of its partner's SFO aggregates. <ul style="list-style-type: none">• Either reissue a takeover of the partner node, setting the -bypass-optimization parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.
Waiting for partner_name. Previous takeover attempt was aborted because reason. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the "-bypass-optimization" parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted because of the reason displayed under reason. The local node owns some of its partner's SFO aggregates. <ul style="list-style-type: none">• Either reissue a takeover of the partner node, setting the -bypass-optimization parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.
Waiting for partner_name. Previous takeover attempt was aborted. Local node owns some of partner's SFO aggregates. Reissue a takeover of the partner with the "-bypass-optimization" parameter set to true to takeover remaining aggregates, or issue a giveback of the partner to return the relocated aggregates.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted. The local node owns some of its partner's SFO aggregates. <ul style="list-style-type: none">• Either reissue a takeover of the partner node, setting the -bypass-optimization parameter to true to takeover the remaining SFO aggregates, or perform a giveback of the partner to return relocated aggregates.

Node State	Description
Connected to partner_name. Previous takeover attempt was aborted because failed to disable background disk firmware update (BDFU) on local node.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because the background disk firmware update on the local node was not disabled.
Connected to partner_name. Previous takeover attempt was aborted because reason.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt was aborted because of the reason displayed under reason.
Waiting for partner_name. Previous takeover attempt was aborted because reason.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt was aborted because of the reason displayed under reason.
Connected to partner_name. Previous takeover attempt by partner_name was aborted because reason.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt by the partner node was aborted because of the reason displayed under reason.
Connected to partner_name. Previous takeover attempt by partner_name was aborted.	The HA interconnect is active and can transmit data to the partner node. The previous takeover attempt by the partner node was aborted.
Waiting for partner_name. Previous takeover attempt by partner_name was aborted because reason.	The local node cannot exchange information with the partner node over the HA interconnect. The previous takeover attempt by the partner node was aborted because of the reason displayed under reason.
Previous giveback failed in module: module name. Auto giveback will be initiated in number of seconds seconds.	<p>The previous giveback attempt failed in module module_name. Auto giveback will be initiated in number of seconds seconds.</p> <ul style="list-style-type: none"> • Run the <code>storage failover show-giveback</code> command for more information.
Node owns partner's aggregates as part of the non-disruptive controller upgrade procedure.	The node owns its partner's aggregates due to the non-disruptive controller upgrade procedure currently in progress.
Connected to partner_name. Node owns aggregates belonging to another node in the cluster.	The HA interconnect is active and can transmit data to the partner node. The node owns aggregates belonging to another node in the cluster.
Connected to partner_name. Waiting for partner lock synchronization.	The HA interconnect is active and can transmit data to the partner node. The system is waiting for partner lock synchronization to complete.

Node State	Description
Connected to partner_name. Waiting for cluster applications to come online on the local node.	The HA interconnect is active and can transmit data to the partner node. The system is waiting for cluster applications to come online on the local node.
Non-HA mode, reboot to use full NVRAM.	<p>Storage failover is not possible. The HA mode option is configured as non_ha.</p> <ul style="list-style-type: none"> • You must reboot the node to use all of its NVRAM.
Non-HA mode. Reboot node to activate HA.	<p>Storage failover is not possible.</p> <ul style="list-style-type: none"> • The node must be rebooted to enable HA capability.
Non-HA mode.	<p>Storage failover is not possible. The HA mode option is configured as non_ha.</p> <ul style="list-style-type: none"> • You must run the <code>storage failover modify -mode ha -node nodename</code> command on both nodes in the HA pair and then reboot the nodes to enable HA capability.

Commands for enabling and disabling storage failover

Use the following commands to enable and disable storage failover functionality.

If you want to...	Use this command...
Enable takeover	<code>storage failover modify -enabled true -node nodename</code>
Disable takeover	<code>storage failover modify -enabled false -node nodename</code>



You should only disable storage failover if required as part of a maintenance procedure. If you have any questions about whether you should disable storage failover, contact NetApp Support.

Documentation for the SnapMirror Business Continuity solution

This site contains the documentation for the NetApp SM-BC solution available with ONTAP 9.8.

Introduction

Overview

Beginning with ONTAP 9.8, you can use SnapMirror Business Continuity (SM-BC) to protect applications with LUNs, enabling applications to fail over transparently, ensuring business continuity in case of a disaster. SM-BC is supported on AFF clusters or All SAN Array (ASA) clusters, where the primary and secondary clusters can be either AFF or ASA. SM-BC protects applications with iSCSI or FCP LUNs.

Benefits

SnapMirror Business Continuity provides the following benefits:

- Provides continuous availability for business-critical applications
- Ability to host critical applications alternately from primary and secondary site
- Simplified application management using consistency groups for dependent write-order consistency
- The ability to test failover for each application
- Instantaneous creation of mirror clones without impacting application availability

Typical use cases

Application deployment for zero RTO or Transparent Application Failover

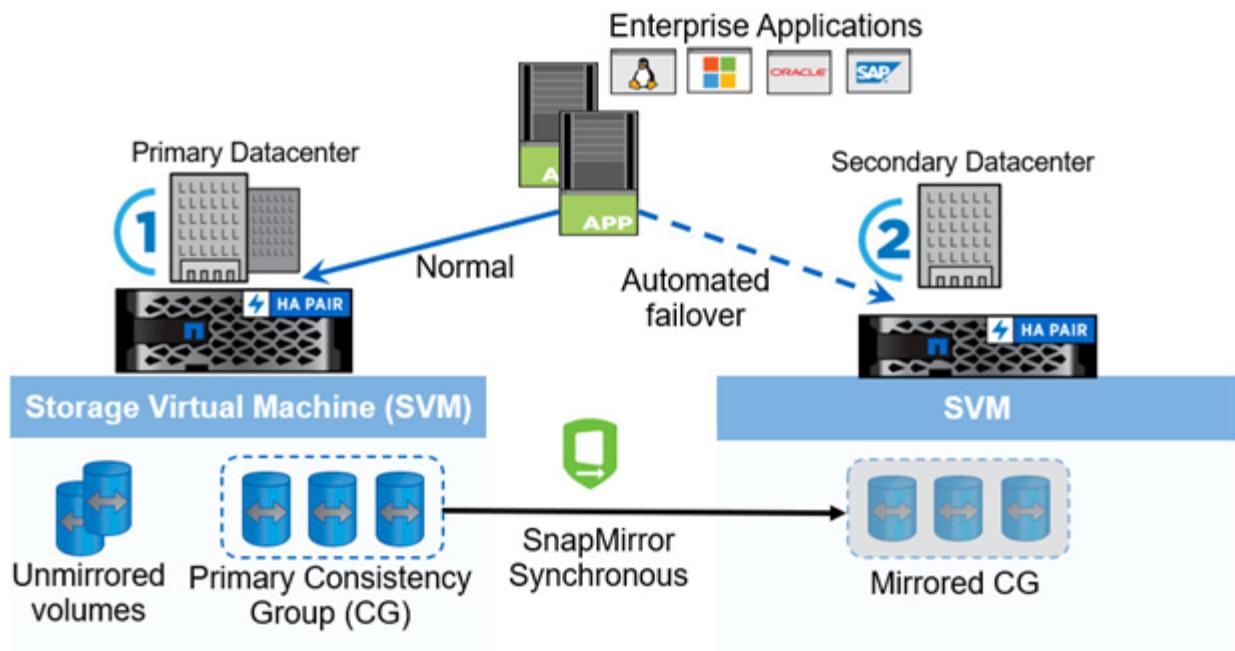
Transparent Application Failover is based on host multipath I/O (MPIO) software-based path failover to achieve non-disruptive access to the storage. Both LUN copies, for example, primary(L1P) and mirror copy(L1S), have the same identity (serial number) and are reported as read-writable to the host. However, reads and writes are serviced only by the primary volume. I/Os issued to the mirror copy are proxied to the primary copy. The host's preferred path to L1 is VS1:N1 based on Asymmetric Logical Unit Access (ALUA) access state Active Optimized (A/O). Mediator is recommended as part of the deployment, primarily to perform failover in case of a storage outage on the primary.

Disaster scenario

The site hosting the primary cluster experiences a disaster. Host multipathing software marks all paths through the cluster as down and uses paths from the secondary cluster. The result is a non-disruptive failover to the mirror copy for LUN L1. L1S is converted from a mirror copy to an active copy of LUN L1. The failover happens automatically when an external Mediator is configured. The host's preferred path to L1 becomes VS2:N1.

Architecture

The following figure illustrates the operation of the SnapMirror Business Continuity feature at a high level.



Key terminology

As you begin to explore the ONTAP SnapMirror Business Continuity and plan a deployment, it is helpful to become familiar with the key terminology and concepts.

SM-BC

Acronym for the SnapMirror Business Continuity (SM-BC) solution available with ONTAP 9.8 and later.

Consistency group

A consistency group (CG) is a collection of FlexVol volumes that provide a write order consistency guarantee for the application workload which needs to be protected for business continuity. The purpose of a consistency group is to take simultaneous crash-consistent Snapshot copies of a collection of volumes at a point in time. In regular deployment, the group of volumes picked to be part of a CG are mapped to an application instance. SnapMirror relationships, also known as a CG relationship, is established between a source CG and a destination CG. The source and destination CGs must contain the same number and type of volumes.

Constituent

The individual FlexVol volumes that are part of a consistency group.

Mediator

External software installed in a standalone server or in a VM. It is a monolithic process that is required to complete a quorum for SM-BC deployment. Mediator is used for health checking and to establish a consensus across a 3-party quorum where the other two parties are the two clusters hosting the SM-BC primary CG and mirror CG copies. Both are used interchangeably.

Out of Sync (OOS)

The application I/O is not replicating to the secondary storage system. The destination volume is not in sync with the source volume because SnapMirror replication is not occurring. If the mirror state is Snapmirrored, this indicates a transfer failure or failure due to an unsupported operation.

Zero RPO

Zero recovery point objective. This is the acceptable amount of data loss from downtime.

Zero RTO

Zero recovery time objective or Transparent Application Failover is achieved by using host multipath I/O (MPIO) software-based path failover to provide non-disruptive access to the storage.

Role of Mediator

ONTAP Mediator provides an alternate health path to the peer cluster, with the intercluster LIFs providing the other health path. With the Mediator's health information, clusters can differentiate between intercluster LIF failure and site failure. When the site goes down, Mediator passes on the health information to the peer cluster on demand, facilitating the peer cluster to fail over. With the Mediator-provided information and the intercluster LIF health check information, ONTAP determines whether to perform an auto failover, if it is failover incapable, continue or stop.

Mediator is one of three parties in the SM-BC quorum, working with the primary cluster and the secondary cluster to reach a consensus. A consensus requires at least two parties in the quorum to agree to an operation.

Basic failover and recovery concepts

It might be helpful to understand some of the basic SM-BC failover and recovery concepts.

Planned failover

A manual operation to change the roles of copies in a SM-BC relationship. The primary becomes the secondary and the secondary becomes the primary. ALUA reporting also changes.

Automatic unplanned failover (AUFO)

An automatic operation to perform a failover to the mirror copy. The operation requires assistance from Mediator to detect that the primary copy is unavailable.

Additional information

For more information about data protection using SnapMirror Synchronous, see the following documentation:

[SnapMirror Synchronous disaster recovery basics](#)

Planning

Prerequisites

There are several prerequisites that you should consider as part of planning a SnapMirror Business Continuity solution deployment.

Hardware

- Only two-node HA clusters are supported

- Both clusters must be either AFF or ASA (no mixing)

Software

- ONTAP 9.8 or later
- ONTAP Mediator 1.2 or later
- A Linux server or virtual machine for the ONTAP Mediator running one of the following:
 - RedHat Enterprise Linux 7.6 or 7.7
 - CentOS 8.0 or 8.1

Licensing

- SnapMirror synchronous (SM-S) license must be applied on both clusters
- SnapMirror license must be applied on both clusters



If your ONTAP storage systems were purchased before June 2019, click [NetApp ONTAP Master License Keys](#) to get the required SM-S license.

Networking environment

- Inter-cluster latency round trip time (RTT) must be less than 10 milliseconds

Supported protocols

- Only SAN protocols are supported (not NFS/CIFS)
- Only Fibre Channel and iSCSI protocols are supported

ONTAP Mediator

- Must be provisioned externally and attached to ONTAP for transparent application failover

Read-write destination volumes

- SM-BC relationships are not supported on read-write destination volumes. Before you can use a read-write volume, you must convert it to a DP volume by creating a volume-level SnapMirror relationship and then deleting the relationship. For details, see [Converting existing relationships to SM-BC relationships](#)

Large LUNs and large volumes

- Large LUNs and large volumes greater than 100TB are supported only on All SAN Arrays



You must ensure that both the primary and secondary cluster are All SAN Arrays, and that they both have ONTAP 9.8 installed. If the secondary cluster is running a version earlier than ONTAP 9.8 or if it is not an All SAN Array, the synchronous relationship can go out of sync if the primary volume grows larger than 100 TB.

AppDM Application volumes

Volumes associated with an AppDM Application are not supported with SM-BC. Before creating an SM-BC relationship for a set of volumes, make sure that none of the volumes are associated with an AppDM Application.



In ONTAP 9.8 RC releases, SM-BC does not automatically check before creating a relationship with a set of AppDM Application volumes.

Additional restrictions and limitations

There are several additional restrictions and limitations when using the SnapMirror Business Continuity solution.

Consistency groups

The maximum number of SnapMirror Synchronous consistency group relationships in a cluster is five, a limit which is platform-independent. If you reach or attempt to exceed this limit, the following message is displayed:

The number of SnapMirror Synchronous consistency group relationships in a cluster cannot exceed 5

Volumes per consistency group

The maximum number of volumes supported per SnapMirror Synchronous consistency group relationship is twelve, a limit which is platform-independent. If you reach or attempt to exceed this limit, the following message is displayed:

The number of volumes in a SnapMirror Synchronous Consistency Group cannot exceed 12

Volumes



The limit is on the number of endpoints and not the number of relationships. A consistency group with 12 volumes contributes 12 endpoints on both the source and destination. A SnapMirror Synchronous relationship with both source and destination volumes on the same HA pair contributes 2 endpoints.

The maximum endpoints per platform are included in the following table.

S. No	Platform	Endpoints per HA for SM-BC	Overall sync and SM-BC endpoints per HA
1	AFF	60	80
2	ASA	60	80

SAN object limits

The following SAN object limits are included in the following table and apply regardless of the platform.

Limits of objects in an SM-BC relationship	Count
LUNs per volume	256
LUN maps per node	2048

Limits of objects in an SM-BC relationship	Count
LUN maps per cluster	4096
LIFs per VServer (with at least one volume in an SM-BC relationship)	256
Inter-cluster LIFs per node	4
Inter-cluster LIFs per cluster	8

NTFS security style

NTFS security style is not supported on SM-BC volumes.

ONTAP access options

You have several access options available when configuring the ONTAP nodes participating in an SM- BC deployment. You should select the option that best matches your specific environment and deployment goals.



In all cases, you must sign in using the administrator account with a valid password.

Command line interface

The text-based command line interface is available through the ONTAP management shell. You can access the CLI using secure shell (SSH).

System Manager

You can connect to the ONTAP System Manager using a modern web browser. The web GUI provides an intuitive and easy-to-use interface when accessing the SnapMirror Business Continuity functionality. For more information about using System Manager, see [ONTAP System Manager documentation](#).

REST API

The ONTAP REST API exposed to external clients provides another option when connecting to the ONTAP. You can access the API using any mainstream programming language or tool that supports REST web services. Popular choices include:

- Python (including the ONTAP Python client library)
- Java
- Curl

Using a programming or scripting language provides an opportunity to automate the deployment and management of a SnapMirror Business Continuity deployment. For more information, see the ONTAP online documentation page at your ONTAP storage system.

Preparing to use the ONTAP CLI

You should be familiar with the following commands when deploying the SnapMirror Business Continuity solution using the ONTAP command line interface.



SM-BC does not support the `snapmirror quiesce` and `snapmirror resume` commands for relationships with active sync policy.

For more information about the following ONTAP commands, see [NetApp Documentation: ONTAP 9](#).

Command	Description
<code>lun igroup create</code>	Create an igroup on a cluster
<code>lun map</code>	Map a LUN to an igroup
<code>lun show</code>	Display a list of LUNs
<code>snapmirror create</code>	Create a new SnapMirror relationship
<code>snapmirror initialize</code>	Initialize an SM-BC consistency group
<code>snapmirror update</code>	Initiates a common snapshot creation operation
<code>snapmirror show</code>	Display a list of SnapMirror relationships
<code>snapmirror failover</code>	Start a planned failover operation
<code>snapmirror resync</code>	Start a resynchronization operation
<code>snapmirror delete</code>	Delete a SnapMirror relationship
<code>snapmirror release</code>	Remove source information for a SnapMirror relationship

Preparing to use the ONTAP Mediator

The ONTAP Mediator establishes a quorum for the ONTAP clusters in an SM-BC relationship. It coordinates automated failover when a failure is detected and helps to avoid split-brain scenarios when each cluster simultaneously tries to establish control as the primary cluster.

Prerequisites for the ONTAP Mediator

The ONTAP Mediator includes its own set of prerequisites. You must meet these prerequisites before installing the mediator. For more information, see [Installing or upgrading the ONTAP Mediator service](#).

Network configuration

By default, the ONTAP Mediator provides service through TCP port 31784. You should make sure that port 31784 is open and available between the ONTAP clusters and the mediator.

Summary of deployment best practices

There are several best practices that you should consider as part of planning an SnapMirror Business Continuity deployment.

SAN

The SnapMirror Business Continuity solution supports only SAN workloads. You should follow the SAN best

practices in all cases.

In addition:

- Replicated LUNs in the secondary cluster must be mapped to the host and the I/O paths to the LUNs from both the primary and secondary cluster must be discovered at the time of host configuration.
- After an out of sync (OOS) event exceeds 80 seconds, or after an automatic unplanned failover, it is important to rescan the host LUN I/O path to ensure that there is no I/O path loss. For more information, see the respective host OS vendor's documentation on rescan of LUN I/O paths.

Mediator

To be fully functional and to enable automatic unplanned failover, the external ONTAP mediator should be provisioned and configured with ONTAP clusters.

When installing the mediator, you should replace the self-signed certificate with a valid certificate signed by a mainstream reliable CA.

SnapMirror

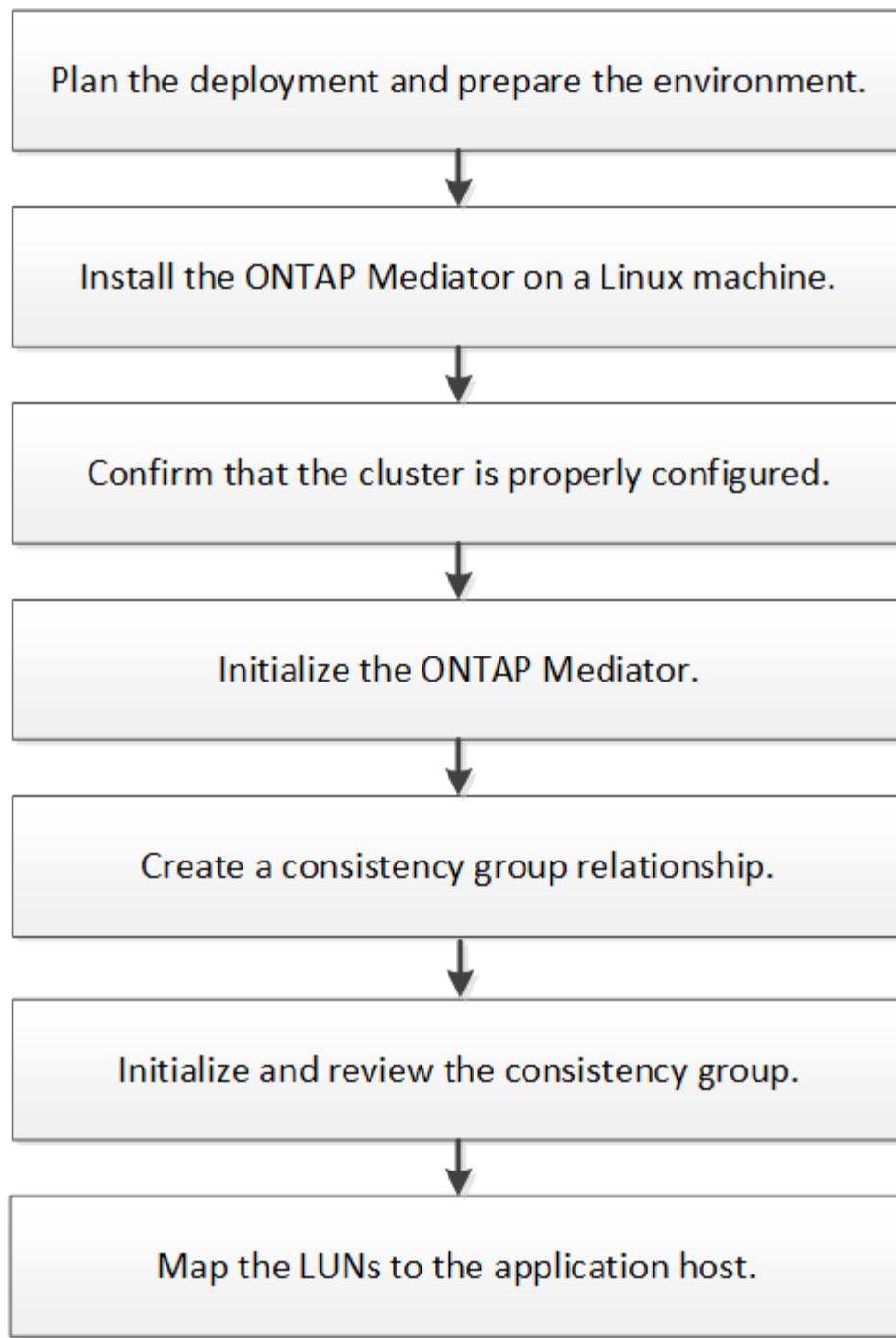
You should terminate an SnapMirror relationship in the following order:

1. Perform `snapmirror delete` at the destination cluster
2. Perform `snapmirror release` at the source cluster

Installation and setup

High level deployment workflow

You can use the following workflow to install and implement the SnapMirror Business Continuity solution.



Installing the ONTAP Mediator

You must install the ONTAP Mediator, which includes accepting the licensing agreement, before you can configure and use the SnapMirror Business Continuity solution.

Before you begin

The following software is required:

- ONTAP Mediator 1.2 or later
- One of the following Linux distributions:
 - RHEL 7.6 or 7.7

- CentOS 8.0 or 8.1

About this task

You should install the ONTAP Mediator at an external site that is physically separated from the two ONTAP clusters.

For complete installation instructions, see [Installing or upgrading the ONTAP Mediator service](#)

Steps

1. Sign into the Linux system that will host the ONTAP Mediator.
2. Download the mediator installation package from the ONTAP Mediator page.

[NetApp Downloads: ONTAP Mediator](#).

3. Install the ONTAP Mediator and respond to all prompts as required:

```
./ontap-mediator_1.2
```

4. Optionally replace the self-signed SSL and certificate authority (CA) with the third party validated SSL Certificate and CA. The certificate you install must not be expired. Copy the contents of the ca.crt file from the ONTAP Mediator directory:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
```

5. At the ONTAP CLI, install the certificate on both the local and peer cluster:

```
security certificate install -type server-ca -vserver cserverName
```

Confirm the ONTAP cluster configuration

You should make sure that your source and destination clusters are configured properly.

About this task

Proceed through each of the following steps. For each step, you should confirm that the specific configuration has been performed. Use the link included after each step to get more information as needed.

Steps

1. Confirm that a cluster peering relationship exists between the clusters.

[Configure peer relationships](#)

2. Confirm that the Storage VMs are created on each cluster.

[Creating an SVM](#)

3. Confirm that a peer relationship exists between the Storage VMs on each cluster.

[Creating an SVM peering relationship](#)

4. Confirm that the volumes exist for your LUNs.

[Creating a volume](#)

5. Confirm that at least one SAN LIF is created on each node in the cluster.

[Considerations for LIFs in a cluster SAN environment](#)

[Creating a LIF](#)

6. Confirm that the necessary LUNs are created and mapped to igroup, which is used to map LUNs to the initiator on the application host.

[Create LUNs and map igroups](#)

7. Rescan the application host to discover any new LUNs.

Initialize the ONTAP Mediator

You must initialize Mediator on one of your cluster peers before SM-BC can perform planned and automatic unplanned failover operations.

About this task

You can initialize Mediator from either cluster. When you issue the `mediator add` command on one cluster, Mediator is automatically added on the other cluster.

Steps

1. Initialize Mediator on one of the clusters:

```
snapmirror mediator add -mediator-address IP_Address -peer-cluster
cluster_name -username user_name
```

Example

```
cluster1::> snapmirror mediator add -mediator-address 192.168.10.1 -peer
-cluster cluster2 -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: *****
Enter the password again: *****
```

2. Check the status of the Mediator configuration:

```
snapmirror mediator show
```

Mediator Address	Peer Cluster	Connection Status	Quorum Status
192.168.10.1	cluster-2	connected	true

`-quorum-status` indicates whether the SnapMirror consistency group relationships are synchronized with Mediator.

Creating a consistency group relationship

You must create a SnapMirror consistency group which also establishes the synchronous consistency group relationship.

Before you begin

The following prerequisites and restrictions apply:

- You must be a cluster or storage VM administrator
- You must have a SnapMirror Synchronous license
- The destination volumes must be type DP
- The primary and the secondary storage VM must be in a peered relationship
- All constituent volumes in a consistency group must be in a single Storage VM
- You cannot establish SM-BC consistency group relationships across ASA clusters and non-ASA clusters

About this task

You must create the consistency group relationship from the destination cluster. You can map up to 12 constituents using the `cg-item-mappings` parameter on the `snapmirror create` command.

Steps

1. Create a consistency group and constituent relationship. This example creates two consistency groups: srccg with constituent volumes vol1 and vol2, and dstcg with constituent volumes vol1_dr and vol2_dr.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailover
```

Initializing a consistency group

After creating a consistency group, you must initialize it.

Before you begin

You must be a cluster or storage VM administrator.

About this task

You initialize the consistency group from the destination cluster.

Steps

1. Sign in to the ONTAP CLI at the destination cluster and initialize the consistency group:

```
destination::>snapmirror initialize -destination-path vs1_dst:/cg/cg_dst
```

2. Confirm that the initialization operation completed successfully. The status should be `InSync`.

```
snapmirror show
```

Mapping LUNs to the application hosts

You must create an igroup on each cluster so you can map LUNs to the initiator on the application host.

About this task

You should perform this configuration on both the source and destination clusters.

Steps

1. Create an igroup on each cluster:

```
lun igroup create -igroup name -protocol fcp|iscsi -ostype os -initiator
initiator_name
```

Example

```
lun igroup create -igroup ig1 -protocol iscsi -ostype linux -initiator
-initiator iqn.2001-04.com.example:abc123
```

2. Map LUNs to the igroup:

```
lun map -path path_name -igroup igroup_name
```

Example:

```
lun map -path /vol/src1/11 -group ig1
```

3. Verify the LUNs are mapped:

```
lun show
```

4. On the application host, discover the new LUNs.

Administration

Creating a common Snapshot copy

In addition to the regularly scheduled Snapshot copy operations, you can manually create a common Snapshot copy between the volumes in the primary SnapMirror consistency group and the volumes in the secondary SnapMirror consistency group.

Before you begin

The SnapMirror group relationship must be in sync.

Steps

1. Create a common Snapshot copy:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Monitor the progress of the update:

```
destination::>snapmirror show -fields -newest-snapshot
```

Performing a planned failover

You can perform a planned failover to test your disaster recovery configuration or to perform maintenance on the primary cluster.

Before you begin

- The relationship must be in sync
- Nondisruptive operations must not be running
- The ONTAP Mediator must be configured, connected, and in quorum

About this task

A planned failover is initiated by the administrator of the secondary cluster. The operation requires switching the primary and secondary roles so that the secondary cluster takes over from the primary. The new primary cluster can then begin processing input and output requests locally without disrupting client operations.

Steps

1. Start the failover operation:

```
destination::>snapmirror failover start -destination-path vs1_dst:/cg/cg_dst
```

2. Monitor the progress of the failover:

```
destination::>snapmirror failover show
```

3. When the failover operation is complete, you can monitor the Synchronous SnapMirror protection relationship status from the destination:

```
destination::>snapmirror show
```

Automatic unplanned failover operations

An automatic unplanned failover (AUFO) operation occurs when the primary cluster is down or isolated. When this occurs, the secondary cluster is converted to the primary and begins serving clients. This operation is performed only with assistance from the ONTAP Mediator.



After the automatic unplanned failover, it is important to rescan the host LUN I/O paths so that there is no loss of I/O paths.

You can monitor the status of the automatic unplanned failover by using the `snapmirror failover show` command.

Basic monitoring

There are several SM-BC components and operations you can monitor.

ONTAP mediator

During normal operation, the Mediator state should be connected. If it is in any other state, this might indicate an error condition. You can review the Event Management System (EMS) messages to determine the error and appropriate corrective actions.

EMS Name	Description
sm.mediator.added	Mediator is added successfully
sm.mediator.removed	Mediator is removed successfully
sm.mediator.unusable	Mediator is unusable due to a corrupted Mediator server
sm.mediator.misconfigured	Mediator is repurposed or the Mediator package is no longer installed on the Mediator server
sm.mediator.unreachable	Mediator is unreachable
sm.mediator.removed.force	Mediator is removed from the cluster using the "force" option
sm.mediator.cacert.expiring	Mediator certificate authority (CA) certificate is due to expire in 30 days or less
sm.mediator.serverc.expiring	Mediator server certificate is due to expire in 30 days or less
sm.mediator.clientc.expiring	Mediator client certificate is due to expire in 30 days or less
sm.mediator.cacert.expired	Mediator certificate authority (CA) certificate has expired
sm.mediator.serverc.expired	Mediator server certificate has expired
sm.mediator.clientc.expired	Mediator client certificate has expired
sm.mediator.in.quorum	All the SM-BC records are resynchronized with Mediator

Planned failover operations

You can monitor status and progress of a planned failover operation using the `snapmirror failover show` command. For example:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Once the failover operation is complete, you can monitor the Synchronous SnapMirror protection status from the new destination cluster. For example:

```
ClusterA::> snapmirror show
```

You can also review the following messages to determine if there is an error and take the appropriate corrective actions.

EMS Name	Description
smbc.pfo.failed	SMBC planned failover operation failed. Destination path:
smbc.pfo.start. Destination path:	SMBC planned failover operation started

Automatic unplanned failover operations

During an unplanned automatic failover, you can monitor the status of the operation using the `snapmirror failover show` command. For example:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
    Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
    Failover Status: completed
    Error Reason:
        End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
    Failover Type: unplanned
    Error Reason codes: -
```

You can also review the following messages to determine if there is an error and take the appropriate corrective actions.

EMS Name	Description
smbc.aupo.failed	SnapMirror automatic planned failover operation failed. Destination path:
smbc.aupo.start. Destination path:	SMBC planned failover operation started
smbc.aupo.completed:	SnapMirror automatic planned failover operation completed. Destination path:
smbc.aupo.failover.incapable	block.giveback.during.aupo

SM-BC availability

You can check the availability of the SM-BC relationship using a series of commands, either on the primary cluster, the secondary cluster, or both.

Commands you use include the `snapmirror mediator show` command on both the primary and secondary cluster to check the connection and quorum status, the `snapmirror show` command, and the `volume show` command. For example:

```

SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86     SMBC_B          connected        true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.236.172.86     SMBC_A          connected        true

SMBC_B::*> snapmirror show -expand

Progress
Source           Destination Mirror Relationship Total
Last
Path             Type   Path       State    Status      Progress Healthy
Updated
-----
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored InSync  -      true   -
vs0:vol1      XDP  vs1:vol1_dp  Snapmirrored InSync  -      true   -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs0      vol1    true        false            Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
-----
vs1      vol1_dp  false       true            No-consensus

```

Adding and removing volumes in a consistency group

If you want to change the composition of the consistency group by adding or removing a volume, you must first delete the original relationship and then create the consistency group again with the new composition.

About this task

- The composition change is not allowed when the consistency group is in the “InSync” state.
- The destination volume should be of type DP.

The new volume you add to expand the consistency group must have a pair of common Snapshot copies between the source and destination volumes.

Steps

This procedure assumes that there are two volume mappings: vol_src1 ↔ vol_dst1 and vol_src2 ↔ vol_dst2, in a consistency group relationship between the end points vs1_src:/cg/cg_src and vs1_dst:/cg/cg_dst.

1. Verify that a common Snapshot copy exists between the source and destination volumes on both the source and destination cluster:

```
source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot snapmirror*
destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot snapmirror*
```

2. If no common Snapshot copy exists, create and initialize a FlexVol SnapMirror relationship:

```
destination::>snapmirror initialize -source-path vs1_src:vol_src3 -destination -path vs1_dst:vol_dst2
```

3. Delete the zero RTO consistency group relationship:

```
destination::>snapmirror delete -destination-path vs1_dst:vol_dst3
```

4. Release the source SnapMirror relationship and retain the common Snapshot copies:

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol_dst3
```

5. Unmap the LUNs and delete the existing consistency group relationship:

```
destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup <igroup_name>
```

NOTE: The destination LUNs are unmapped, while the LUNs on the primary copy continue to serve the host I/O.

```
destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

```
source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst -relationship -info-only true
```

6. Create the new consistency group with the new composition:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src -destination -path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1, vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

7. Resynchronize the zero RTO consistency group relationship to ensure it is in sync:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Remap the LUNs that you unmapped in Step 5:

```
destination::> lun map -vserver vs1_dst -path <lun_path> -igroup <igroup_name>
```

9. Rescan host LUN I/O paths to restore all paths to the LUNs.

Converting existing relationships to SM-BC relationships

You can convert an existing zero recovery point protection (zero RPO) Synchronous SnapMirror relationship to an SM-BC zero RTO Synchronous SnapMirror consistency group relationship.

Before you begin

- A zero RPO Synchronous SnapMirror relationship exists between the primary and secondary
- All LUNs on the destination volume are unmapped before the zero RTO SnapMirror relationship is created

About this task

- You must be a cluster and SVM administrator on the source and destination.
- You cannot convert zero RPO to zero RTO sync by changing the SnapMirror policy.
- If existing LUNs on the secondary volume are mapped, `snapmirror create` with AutomatedFailover policy triggers an error.
You must ensure the LUNs are unmapped before issuing the `snapmirror create` command.

Steps

1. Perform a SnapMirror update operation on the existing relationship:

```
destination::>snapmirror update -destination-path vs1_dst:vol1
```

2. Verify that the SnapMirror update completed successfully:

```
destination::>snapmirror show
```

3. Quiesce each of the zero RPO synchronous relationships:

```
destination::>snapmirror quiesce -destination-path vs1_dst:vol1
```

```
destination::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. Delete each of the zero RPO synchronous relationships:

```
destination::>snapmirror delete -destination-path vs1_dst:vol1
```

```
destination::>snapmirror delete -destination-path vs1_dst:vol2
```

5. Release the source SnapMirror relationship but retain the common Snapshot copies:

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol1
```

```
source::>snapmirror release -relationship-info-only true -destination-path vs1_dst:vol2
```

6. Create a group zero RTO Synchronous Snapmirror relationship:

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy AutomatedFailover
```

7. Resynchronize the zero RTO consistency group:

```
destination::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

8. Rescan host LUN I/O paths to restore all paths to the LUNs.

SM-BC upgrade and revert considerations

You should be aware of the requirements for upgrading and reverting an SM-BC configuration.

Upgrade

Before you can configure and use SM-BC, you must upgrade all nodes on the source and destination clusters to ONTAP 9.8 or later.

[Upgrading software on ONTAP clusters](#)



SM-BC is not supported with mixed ONTAP 9.7 and ONTAP 9.8 clusters.

Reverting to ONTAP 9.7 from ONTAP 9.8

When you revert from ONTAP 9.8 to ONTAP 9.7, you must be aware of the following:

- If the cluster is hosting an SM-BC destination, reverting to ONTAP 9.7 is not allowed until the relationship is broken and deleted.
- If the cluster is hosting an SM-BC source, reverting to ONTAP 9.7 is not allowed until the relationship is released.
- All user-created custom SM-BC SnapMirror policies must be deleted before reverting to ONTAP 9.7.

Steps

1. Perform a revert check from one of the clusters in the SM-BC relationship:

```
cluster::*> system node revert-to -version 9.7 -check-only
```

Example:

```
cluster::*> system node revert-to -version 9.7 -check-only
Error: command failed: The revert check phase failed. The following
issues must be resolved before revert can be completed. Bring the data
LIFs down on running vservers. Command to list the running vservers:
vserver show -admin-state running Command to list the data LIFs that are
up: network interface show -role data -status-admin up Command to bring
all data LIFs down: network interface modify {-role data} -status-admin
down
Disable snapshot policies.

Command to list snapshot policies: "snapshot policy show".
```

```
    Command to disable snapshot policies: "snapshot policy modify  
-vserver  
* -enabled false"

    Break off the initialized online data-protection (DP) volumes and  
delete  
    Uninitialized online data-protection (DP) volumes present on the  
local  
node.  
    Command to list all online data-protection volumes on the local  
node:  
        volume show -type DP -state online -node <local-node-name>  
        Before breaking off the initialized online data-protection volumes,  
        quiesce and abort transfers on associated SnapMirror relationships  
and  
        wait for the Relationship Status to be Quiesced.  
        Command to quiesce a SnapMirror relationship: snapmirror quiesce  
        Command to abort transfers on a SnapMirror relationship: snapmirror  
abort  
        Command to see if the Relationship Status of a SnapMirror  
relationship  
        is Quiesced: snapmirror show  
        Command to break off a data-protection volume: snapmirror break  
        Command to break off a data-protection volume which is the  
destination  
        of a SnapMirror relationship with a policy of type "vault":  
snapmirror  
        break -delete-snapshots  
        Uninitialized data-protection volumes are reported by the  
"snapmirror  
        break" command when applied on a DP volume.  
        Command to delete volume: volume delete

        Delete current version snapshots in advanced privilege level.  
        Command to list snapshots: "snapshot show -fs-version 9.8"  
        Command to delete snapshots: "snapshot prepare-for-revert -node  
<nodename>"

        Delete all user-created policies of the type active-strict-sync-  
mirror  
        and active-sync-mirror.  
        The command to see all active-strict-sync-mirror and active-sync-  
mirror  
        type policies is:  
            snapmirror policy show -type  
active-strict-sync-mirror,active-sync-mirror
```

The command to delete a policy is :

```
snapmirror policy delete -vserver <vserver-name> -policy <policy-name>
```

For information on reverting clusters, see [Revert ONTAP](#).

Removing an SM-BC configuration

You can remove zero RTO Synchronous SnapMirror protection and delete the SM-BC relationship configuration.

About this task

Before you delete the SM-BC relationship, all LUNs in the destination cluster must be unmapped.

After the LUNs are unmapped and the host is rescanned, the SCSI target notifies the hosts that the LUN inventory has changed. The existing LUNs on the zero RTO secondary volumes change to reflect a new identity after the zero RTO relationship is deleted. Hosts discover the secondary volume LUNs as new LUNs that have no relationship to the source volume LUNs.

The secondary volumes remain DP volumes after the relationship is deleted. You can issue the snapmirror break command to convert them to read/write.

Deleting the relationship is not allowed in the failed-over state when the relationship is not reversed.

Steps

1. Delete the SM-BC consistency group relationship:

```
Destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
```

2. From the source cluster, release the consistency group relationship and the Snapshot copies created for the relationship:

```
Source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
```

3. Perform a host rescan to update the LUN inventory.

Removing ONTAP Mediator

If you want to remove an existing ONTAP Mediator configuration from your ONTAP clusters, you can do so by using the `snapmirror mediator remove` command.

Steps

1. Remove ONTAP Mediator:

```
snapmirror mediator remove -mediator-address 12.345.678.90 -peer-cluster cluster_xyz
```

Troubleshooting

SnapMirror delete operation fails in takeover state

Issue:

When ONTAP 9.9.1 is installed on a cluster, executing the `snapmirror delete` command fails when an SM-BC consistency group relationship is in takeover state.

Example:

```
C2_cluster::> snapmirror delete vs1:/cg/dd  
  
Error: command failed: RPC: Couldn't make connection
```

Solution

When the nodes in an SM-BC relationship are in takeover state, perform the SnapMirror delete and release operation with the "-force" option set to true.

Example:

```
C2_cluster::> snapmirror delete vs1:/cg/dd -force true  
  
Warning: The relationship between source "vs0:/cg/ss" and destination  
"vs1:/cg/dd" will be deleted, however the items of the  
destination  
    Consistency Group might not be made writable, deletable, or  
modifiable  
    after the operation. Manual recovery might be required.  
Do you want to continue? {y|n}: y  
Operation succeeded: snapmirror delete for the relationship with  
destination "vs1:/cg/dd".
```

Failure creating a SnapMirror relationship and initializing consistency group

Issue:

Creation of SnapMirror relationship and consistency group initialization fails.

Error message:

```
command failed: The number of SnapMirror Synchronous Consistency Group  
relationships in a cluster cannot exceed 5
```

Solution:

Ensure that the configuration has no more than 5 consistency groups. See [Additional restrictions and limitations](#).

Planned failover unsuccessful

Issue:

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicates that a nondisruptive operation is in progress.

Example:

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
08:35:04
08:35:04
```

Cause:

Planned failover cannot begin when a nondisruptive operation is in progress, including volume move, aggregate relocation, and storage failover.

Solution:

Wait for the nondisruptive operation to complete and try the failover operation again.

Mediator not reachable or Mediator quorum status is false

Issue:

After executing the `snapmirror failover start` command, the output for the `snapmirror failover show` command displays a message indicating that Mediator is not configured.

See [Initialize the ONTAP Mediator](#).

Example:

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-----
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Cause:

Mediator is not configured or there are network connectivity issues.

Solution:

If Mediator is not configured, you must configure Mediator before you can establish an SM-BC relationship. Fix any network connectivity issues. Make sure Mediator is connected and quorum status is true on both the source and destination site using the snapmirror mediator show command.

Example:

```
cluster::> snapmirror mediator show
Mediator Address  Peer Cluster      Connection Status Quorum Status
-----
10.234.10.143    cluster2          connected        true
```

Automatic unplanned failover not triggered on Site B

Issue:

A failure on Site A does not trigger an unplanned failover on Site B.

Possible cause #1:

Mediator is not configured. To determine if this is the cause, issue the `snapmirror mediator show` command on the Site B cluster.

Example:

```
Cluster2::*> snapmirror mediator show
This table is currently empty.
```

This example indicates that Mediator is not configured on Site B.

Solution:

Ensure that Mediator is configured on both clusters, that the status is connected, and quorum is set to True.

Possible cause #2:

SnapMirror consistency group is out of sync. To determine if this is the cause, view the event log to view if the consistency group was in sync during the time at which the Site A failure occurred.

Example:

```
cluster::>*> event log show -event *out.of.sync*
```

Time	Node	Severity	Event
10/1/2020 23:26:12	sti42-vsim-ucs511w	ERROR	sms.status.out.of.sync: Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume "vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb- ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason: "Transfer failed."

Solution:

Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the `force` option.
3. Enter the `snapmirror break` command on the consistency group constituent volumes to convert volumes from DP to R/W, to enable I/O from Site B.
4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
5. Release the consistency group with `relationship-info-only` on Site A to retain common Snapshot copy and unmap the LUNs belonging to the consistency group.
6. Convert volumes on Site A from R/W to DP by setting up a volume level relationship using either the Sync policy or Async policy.
7. Issue the `snapmirror resync` to synchronize the relationships.
8. Delete the SnapMirror relationships with the Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using `relationship-info-only true` on Site B.
10. Create a consistency group relationship from Site B to Site A.
11. Perform a consistency group resync from Site A, and then verify that the consistency group is in sync.
12. Rescan host LUN I/O paths to restore all paths to the LUNs.

Link between Site B and Mediator down and Site A down

Example:

```
cluster::>*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.237.86.17      C1_cluster      unreachable      true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::>*> snapmirror show -expand
Source          Destination Mirror Relationship Total
Last
Path           Type   Path       State   Status      Progress Healthy
Updated
-----
-----
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::>*> cluster peer show
Peer Cluster Name      Cluster Serial Number Availability
Authentication
-----
-----
C1_cluster            1-80-000011      Unavailable      ok
```

Solution

Force a failover to enable I/O from Site B and then establish a zero RTO relationship from Site B to Site A.

Complete the following steps to perform a forced failover on Site B.

1. Unmap all LUNs belonging to the consistency group from Site B.
2. Delete the SnapMirror consistency group relationship using the force option.
3. Enter the snapmirror break command on the consistency group constituent volumes to convert volumes from DP to RW, to enable I/O from Site B.
4. Boot up the Site A nodes to create a zero RTO relationship from Site B to Site A.
5. Release the consistency group with relationship-info-only on Site A to retain common Snapshot copy and unmap the LUNs belonging to the consistency group.

6. Convert volumes on Site A from RW to DP by setting up a volume level relationship using either Sync policy or Async policy.
7. Issue the snapmirror resync to synchronize the relationships.
8. Delete the SnapMirror relationships with Sync policy on Site A.
9. Release the SnapMirror relationships with Sync policy using relationship-info-only true on Site B.
10. Create a consistency group relationship from Site B to Site A.
11. Perform a consistency group resync from Site A, and then verify that the consistency group is in sync.
12. Rescan host LUN I/O paths to restore all paths to the LUNs.

Link between Site A and Mediator down and Site B down

Determining the cause:

Check the status of Mediator from Site A.

Example:

```
C1_cluster::>*> snapmirror mediator show
Mediator Address Peer Cluster      Connection Status Quorum Status
-----
10.237.86.17    C2_cluster        unreachable      true

C1_cluster::>*> snapmirror list-destinations
                                         Progress
Source          Destination          Transfer   Last
Relationship
Path            Type   Path          Status  Progress   Updated     Id
-----
-----
vs0:/cg/src_cg_1  XDP    vs1:/cg/dst_cg_1  OutOfSync -           -
bba7d354-06f6-11eb-9138-005056acec19
```

Check Site B connectivity:

```
C1_sti78-vs1m-ucs188a_cluster::>*> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability
Authentication
-----
-----
C2_cluster                  1-80-000011          Unavailable      ok
```

Check the consensus status on SM-BC volume:

```
C1_cluster::*> volume show zrto_cg_894191_188b_RW1 -fields smbc-consensus
vserver volume                         smbc-consensus
-----
vs0      zrto_cg_894191_188b_RW1 Awaiting-consensus
```

Solution:

Complete the following steps to override SM-BC consensus and forcefully resume I/O on Site A:

1. Unmap the LUNs on Site A.
2. Issue the snapmirror release command using the `-force` and `override-smbc-consensus` option on Site A.
3. Remap the LUNs.
4. First, bring up Mediator, and then bring up the Site B nodes.
5. Resync the consistency group relationship using `snapmirror resync`.
6. After Site B is up, verify that the consistency group relationship is up and is in sync.
7. Perform a LUN rescan on the host to restore all paths to the LUNs.

SM-BC SnapMirror delete operation fails when fence is set on destination volume

Issue:

SnapMirror delete operation fails when any of the destination volumes have redirection fence set.

Solution

Performing the following operations to retry the redirection and remove the fence from the destination volume.

- SnapMirror resync
- SnapMirror update

Volume move operation stuck when primary is down

Issue:

A volume move operation is stuck indefinitely in cutover deferred state when the primary site is down in an SM-BC relationship.

When the primary site is down, the secondary site performs an automatic unplanned failover (AUFO). When a volume move operation is in progress when the AUFO is triggered the volume move becomes stuck.

Solution:

Abort the volume move instance that is stuck and restart the volume move operation.

SnapMirror release fails when unable to delete Snapshot copy

Issue:

The SnapMirror release operation fails when the Snapshot copy cannot be deleted.

Solution:

The Snapshot copy contains a transient tag. Use the `snapshot delete` command with the `-ignore-owners` option to remove the transient Snapshot copy.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true
```

Retry the `snapmirror release` command.

Volume move reference Snapshot copy shows as the newest

Issue:

After performing a volume move operation on a consistency group volume, the volume move reference Snapshot copy might display as the newest for the SnapMirror relationship.

You can view the newest Snapshot copy with the following command:

```
snapmirror show -fields newest-snapshot status -expand
```

Solution:

Manually perform a `snapmirror resync` or wait for the next automatic resync operation after the volume move operation completes.

Provision SAN storage

The topics in this section show you how to configure and manage SAN environments with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage SAN environments, see this content:

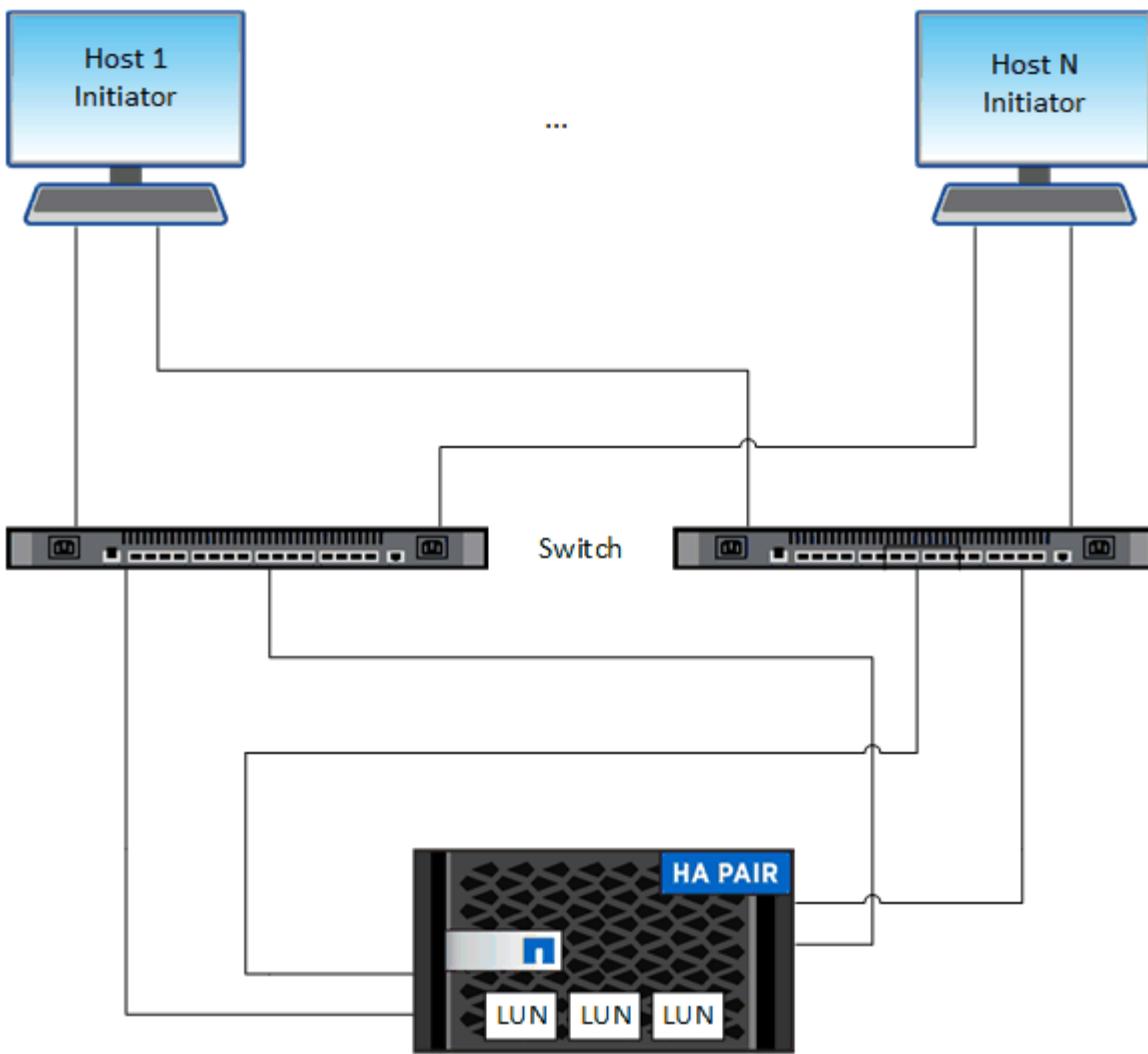
- [SAN Administration Guide](#)
- [SAN Configuration Guide](#)

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to configure and manage SAN protocols on host virtual machines, see this content:

- [FC Configuration for ESXi® using VSC Express Guide](#)
- [FC Configuration for Red Hat® Enterprise Linux® Express Guide](#)
- [FC Configuration for Windows® Express Guide](#)
- [iSCSI Configuration for ESXi® using VSC Express Guide](#)
- [iSCSI Configuration for Red Hat® Enterprise Linux® Express Guide](#)
- [iSCSI Configuration for Windows® Express Guide](#)

SAN overview

You can use the iSCSI and FC protocols to provide storage in a SAN environment.



With iSCSI and FC, storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. You create LUNs and then map them to initiator groups (igroups). Initiator groups are tables of FC host WWPs and iSCSI host node names and control which initiators have access to which LUNs.

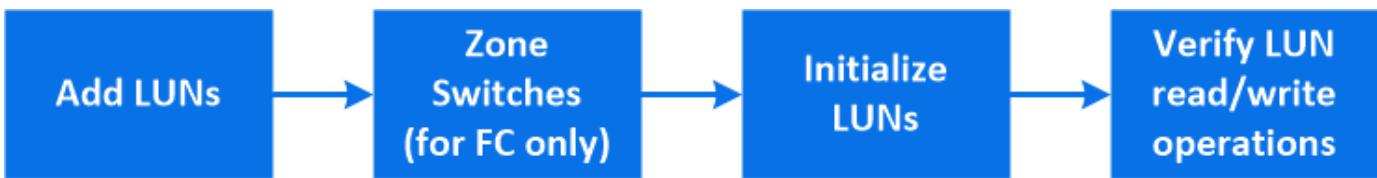
FC targets connect to the network through FC switches and host-side adapters and are identified by world-wide port names (WWPNs). iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

Learn more about [SAN](#).

Provision SAN storage for VMware datastores

Create LUNs to provide storage for an ESXi host using the FC or iSCSI SAN protocol. LUNs appear as disks to the ESXi host.

This procedure creates new LUNs on an existing storage VM. Your FC or iSCSI protocol should already be set up.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. In ONTAP System Manager, click **Storage > LUNs** and then click Add.
 - a. If you need to add an initiator group, click **More Options**.

Beginning in ONTAP 9.9.1, under **HOST INFORMATION**, you have the additional option to create a **New initiator group using existing initiator groups**. This option allows you to create an igroup that consists of other existing igroups.



The OS type for an igroup containing other igroups cannot be changed after it has been created.

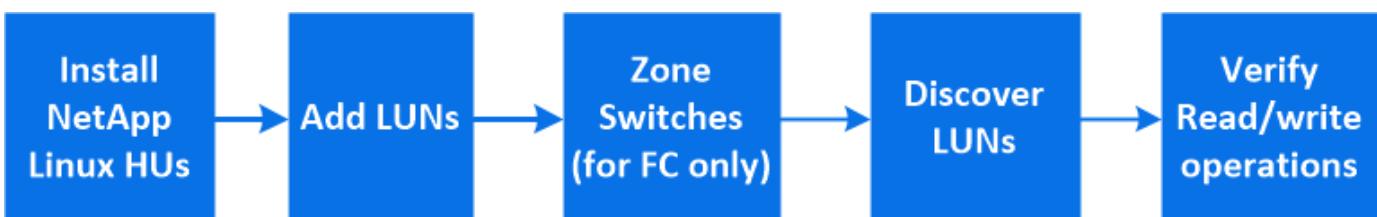
Beginning in ONTAP 9.9.1, you also have the option to add a description to your igroup or host initiator. The description serves as an alias for the igroup or host initiator.

- b. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.
2. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
 3. Use Virtual Storage Console (VSC) for VMware vSphere, to discover and initialize the LUN and to verify that the ESXi hosts can write and read data on the LUN.

Provision SAN storage for Linux servers

Create LUNs to provide storage for a Linux server using the FC or iSCSI SAN protocol. LUNs appear to Linux as SCSI disk devices.

This procedure creates new LUNs on an existing storage VM. Your FC or iSCSI protocol should already be set up. You need to know the initiator identifiers (FC WWPN or iSCSI iqn) for your Linux server.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. On your Linux server, install the [NetApp Linux Host Utilities](#) package.
2. In ONTAP System Manager, click **Storage > LUNs** and then click Add.
 - a. If you need to add an initiator group, click **More Options**.

Beginning in ONTAP 9.9.1, under **HOST INFORMATION**, you have the additional option to create a **New initiator group using existing initiator groups**. This option allows you to create an igrup that consists of other existing igrups.



The OS type for an igrup containing other igrups cannot be changed after it has been created.

Beginning in ONTAP 9.9.1, you also have the option to add a description to your igrup or host initiator. The description serves as an alias for the igrup or host initiator.

- b. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.
3. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
4. On your Linux server, discover the new LUNs:

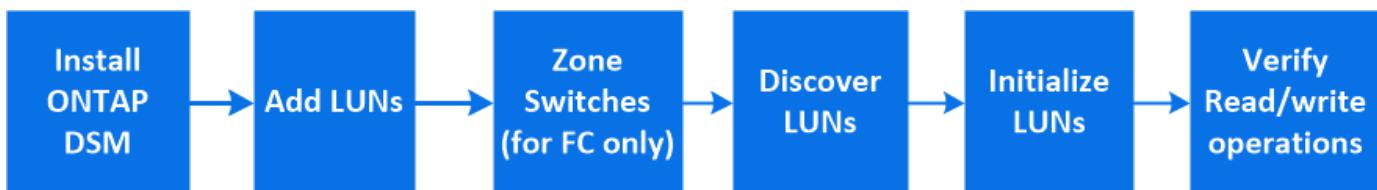
```
/usr/bin/rescan-scsi-bus.sh
```

5. Optionally partition the LUNs and create file systems.
6. Verify the Linux server can write and read data on the LUN.

Provision SAN storage for Windows servers

Create LUNs to provide storage for a Windows server using the FC or iSCSI SAN protocol. LUNs appear as disks to the Windows host.

This procedure creates new LUNs on an existing storage VM. Your FC or iSCSI protocol should already be set up.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. On your Windows server, install Data ONTAP DSM for Windows MPIO.
2. In ONTAP System Manager, click **Storage > LUNs** and then click Add.
 - a. If you need to add an initiator group, click **More Options**.

Beginning in ONTAP 9.9.1, under **HOST INFORMATION**, you have the additional option to create a **New initiator group using existing initiator groups**. This option allows you to create an igrup that consist of other existing igroups.



The OS type for an igrup containing other igroups cannot be changed after it has been created.

Beginning in ONTAP 9.9.1, you also have the option to add a description to your igrup or host initiator. The description serves as an alias for the igrup or host initiator.

- b. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

3. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
4. On your Windows server, discover the new LUN.
5. Initialize the LUN and optionally format it with a file system.
6. Verify the Windows server can write and read data on the LUN.

Create nested igrup

Beginning in ONTAP 9.9.1, you can create an igrup that consists of other existing igroups.

1. In ONTAP System Manager, click **Host > SAN Initiator Groups**, and then click **Add**.
2. Enter the igrup **Name** and **Description**.

The description serves as the igrup alias.

3. Select the **Storage VM** and **Host Operating System**.



The OS type of a nested igrup cannot be changed after the igrup is created.

4. Under **Initiator Group Members** select **Existing initiator group**.

You can use **Search** to find and select the initiator groups you want to add.

Map igroups to multiple LUNs

Beginning in ONTAP 9.9.1, you can map igroups to two or more LUNs simultaneously.

1. In ONTAP System Manager, click **Storage > LUNs**.
2. Select the LUNs you want to map.
3. Click **More**, then click **Map To Initiator Groups**.



The selected igroups are added to the selected LUNs. The pre-existing mappings are not overwritten.

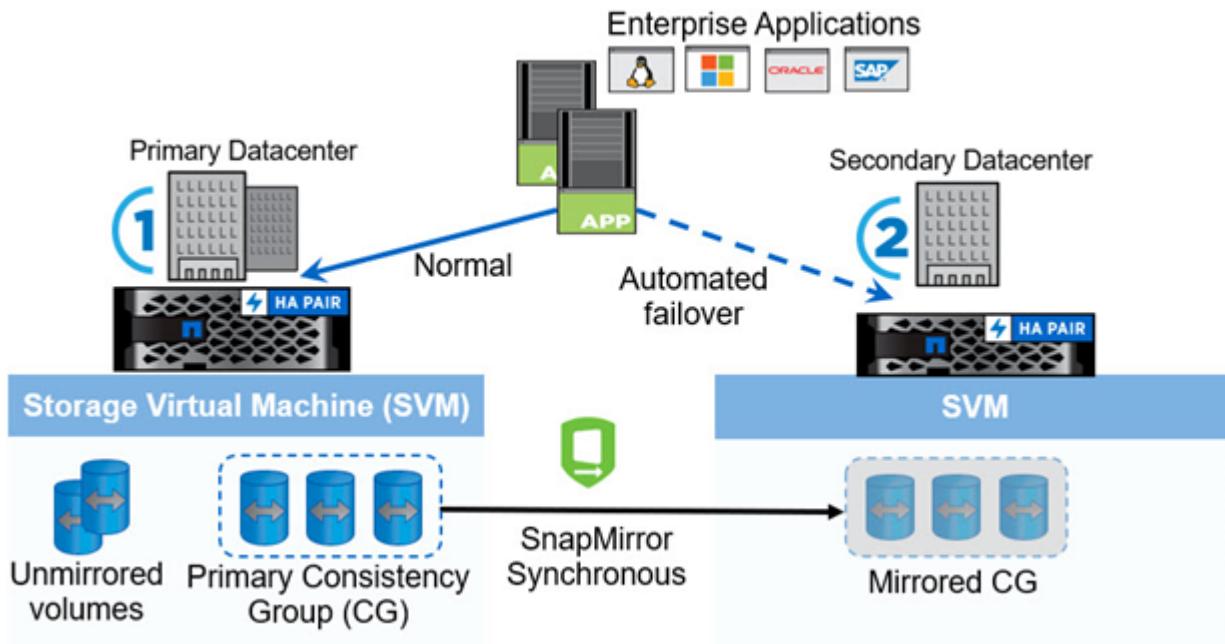
SnapMirror Business Continuity

SnapMirror Business Continuity overview

Starting in ONTAP 9.8, you can use System Manager to protect LUNs for transparent application failover, enabling applications to fail over automatically for business continuity when using two AFF clusters or two All SAN Array (ASA) clusters. Your clusters cannot be mixed; they must consist of two AFF clusters or two ASA clusters. Protection for business continuity supports iSCSI and FCP protocols.

The SnapMirror Business Continuity provides the following benefits:

- Automated failover of business-critical applications
- Simplified application management, using consistency groups for dependent write-order consistency
- The ability to test failover for each application
- Instantaneous creation of mirror clones without impacting application availability



Requirements

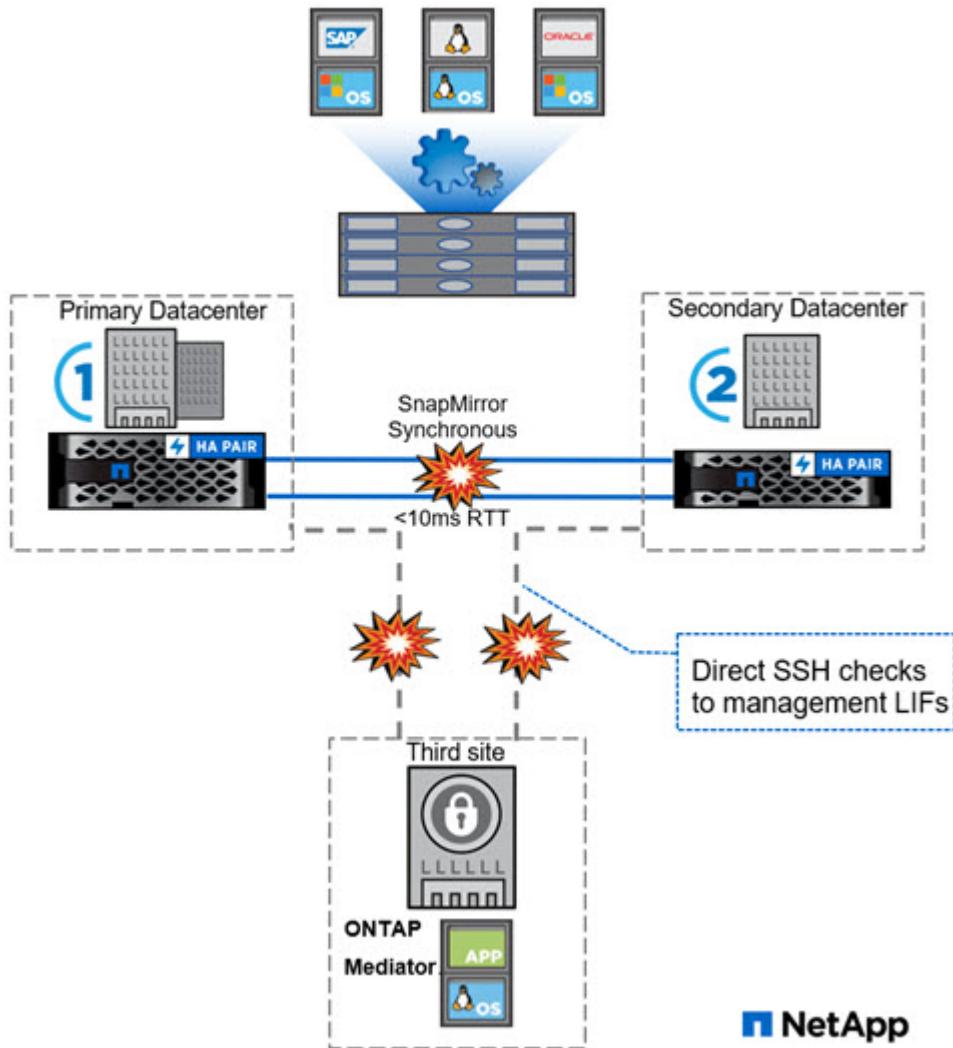
SnapMirror Business Continuity has the following requirements:

- 2-node HA cluster, only – both either AFF or ASA. No intermixing.
- A server or VM running RHEL 7.6 or 7.8 or CentOS 8.0 or 8.1 for installing ONTAP Mediator
- Data Protection or Premium bundle license

Support

SnapMirror Business Continuity provides support for the following:

- Synchronous replication
- SAN protocol – FCP or iSCSI
- Up to 5 consistency groups, each with up to 12 volumes
- A total of 80 concurrent synchronous relationships per HA pair, including consistency groups



Configure Mediator

Use System Manager to configure the Mediator server to be used for automated failover. You can also replace the self-signed SSL and CA with the third party validated SSL Certificate and CA if you have not already done so.

Steps

1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Click **Add**, and enter the following Mediator server information:
 - IPv4 address
 - Username
 - Password

- Certificate

Configure protection for business continuity

Configuring protection for business continuity involves selecting LUNs on the ONTAP source cluster and adding them to a consistency group. Open System Manager from a browser on the source cluster to begin configuring protection for business continuity.

About this task

- LUNs must reside on the same storage VM.
- LUNs can reside on different volumes.
- The source and destination cluster cannot be the same.

Steps

1. Choose the LUNs you want to protect and add them to a protection group: **Protection > Overview > Protect for Business Continuity > Protect LUNs**.
2. Select one or more LUNs to protect on the source cluster.
3. Select the destination cluster and SVM.
4. **Initialize relationship** is selected by default. Click **Save** to begin protection.
5. Go to **Dashboard > Performance** to verify IOPS activity for the LUNs.
6. On the destination cluster, use System Manager to verify that the protection for business continuity relationship is in sync: **Protection > Relationships**.

Reestablish the original protection relationship after an unplanned failover

ONTAP uses the ONTAP Mediator to detect when a failure occurs on the primary storage system and executes automatic unplanned failover to the secondary storage system. You can use ONTAP System Manager to reverse the relationship and reestablish the original protection relationship when original source cluster is back online.

Steps

1. Navigate to **Protection > Relationships** and wait for the relationship state to show “InSync.”
2. To resume operations on the original source cluster, click  and select **Failover**.

Provision NVMe storage

The topics in this section show you how to configure and manage NVMe with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage NVMe, see this content:

- [SAN Administration Guide](#)
- [SAN Configuration Guide](#)

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to configure and manage NVMe, see the content for your ONTAP release:

- [Cluster management using System Manager 9.6 and 9.7](#)
- [Cluster management using System Manager 9.5](#)
- [Cluster management using System Manager 9.3 and 9.4](#)
- [Cluster management using System Manager 9.2 and earlier](#)

NVMe overview

You can use the non-volatile memory express (NVMe) protocol to provide storage in a SAN environment. The NVMe protocol is optimized for performance with solid state storage.

For NVMe, storage targets are called namespaces. An NVMe namespace is a quantity of non-volatile storage that can be formatted into logical blocks and presented to a host as a standard block device. You create namespaces and subsystems, and then map the namespaces to the subsystems, similar to the way LUNs are provisioned and mapped to igroups for FC and iSCSI.

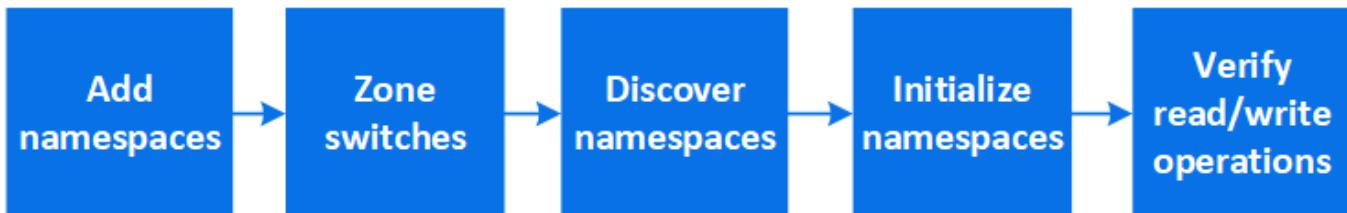
NVMe targets are connected to the network through a standard FC infrastructure using FC switches and host-side adapters.

Learn more about [NVMe](#).

Provision NVMe storage for SUSE Linux

Create namespaces to provide storage for a SUSE Linux server using the NVMe protocol. Namespaces appear to Linux as SCSI disk devices.

This procedure creates new namespaces on an existing storage VM. Your storage VM must be configured for NVME, and your FC transport should already be set up.





Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. In ONTAP System Manager, click **Storage > NVMe Namespaces** and then click **Add**.

If you need to create a new subsystem, click **More Options**.

- a. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

1. Zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
2. On your Linux server, discover the new namespaces.
3. Initialize the namespace and optionally format it with a file system.
4. Verify the Linux server can write and read data on the namespace.

Provision NAS storage

The topics in this section show you how to configure and manage NAS environments with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage NAS environments, see this content:

- [NFS Configuration Power Guide](#)
- [NFS Reference](#)
- [SMB/CIFS and NFS Auditing and Security Tracing Guide](#)
- [SMB/CIFS Configuration Power Guide](#)
- [SMB/CIFS Configuration Guide for Microsoft Hyper-V and SQL Server](#)
- [SMB/CIFS Reference](#)

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to configure and manage NAS protocols, see this content:

- [NFS Configuration Express Guide](#)
- [NFS Configuration for ESXi using VSC Express Guide](#)
- [SMB/CIFS and NFS Multiprotocol Configuration Express Guide](#)
- [SMB/CIFS Configuration Express Guide](#)

NAS overview for ONTAP System Manager

ONTAP enables you to serve data to Linux and Windows clients simply, securely, and efficiently.

ONTAP System Manager supports workflows for:

- Initial configuration of clusters that you intend to use for NAS file services.
- Additional volume provisioning for changing storage needs.
- Configuration and maintenance for industry-standard authentication and security facilities.

Using ONTAP System Manager, you can manage NAS services at the component level:

- Protocols – NFS, SMB/CIFS, or both (NAS multiprotocol)
- Name services – DNS, LDAP, and NIS
- Name service switch
- Kerberos security
- Exports and shares
- Qtrees
- Name mapping of users and groups

Provision NAS storage for VMware datastores

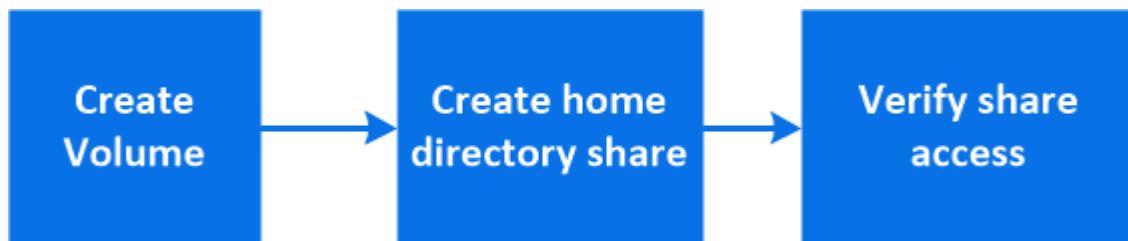
Create volumes to provide VMware datastores using the NFS protocol.

See the [NFS Configuration for ESXi using VSC Express Guide](#) for VMware datastore provisioning best practices.

Provision NAS storage for home directories

Create volumes to provide storage for home directories using the SMB/CIFS protocol.

This procedure creates new volumes for home directories on an [existing SMB-enabled storage VM](#).



Steps

1. In ONTAP System Manager, click **Storage > Volumes** and then click **Add**.
2. Click **Storage > Shares**, click **Add**, and select **Home Directory**.
3. On a Windows client, do the following to verify that the share is accessible.
 - a. In Windows Explorer, map a drive to the share in the following format:
`__SMB_Server_Name__Share_Name__`
If the share name was created with variables (%w, %d, or %u), be sure to test access with a resolved name.
 - b. On the newly created drive, create a test file, and then delete the file.

Provision NAS storage for Linux servers using NFS

Create volumes to provide storage for Linux servers using the NFS protocol.

This procedure creates new volumes on an [existing NFS-enabled storage VM](#).



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. In ONTAP System Manager, click **Storage > Volumes** and then click **Add**.

The default export policy grants full access to all users. You can add more restrictive rules to the export policy later.

.. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

1. On a Linux client, do the following to verify access.
 - a. Create and mount the volume using the network interface of the storage VM.

- b. On the newly mounted volume, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the volume's export policy](#) and set any desired UNIX ownership and permissions on the mounted volume.

Manage access using export policies

Enable Linux client access to NFS servers by using export policies.

This procedure creates or modifies export policies for an [existing NFS-enabled storage VM](#).

Steps

1. In ONTAP System Manager, Click **Storage > Volumes**.
2. Click an NFS-enabled volume and click **More**.
3. Click **Edit Export Policy** and then click **Select an existing policy** or **Add a new policy**.

Provision NAS storage for Windows servers using SMB/CIFS

Create volumes to provide storage for Windows servers using the SMB/CIFS protocol.

This procedure creates new volumes on an [existing SMB-enabled storage VM](#).



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. In ONTAP System Manager, click **Storage > Volumes** and then click **Add**.

The default share grants full access to all users. You can modify the Access Control List (ACL) later.

.. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

1. Switch to a Windows client to verify that the share is accessible.
 - a. In Windows Explorer, map a drive to the share in the following format:
`__SMB_Server_Name__Share_Name__`
 - b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the share ACL](#) and set any desired security properties on the mapped drive.

Provision NAS storage for both Windows and Linux using both NFS and SMB/CIFS

Create volumes to provide storage for clients using either the NFS or SMB/CIFS protocol.

This procedure creates new volumes on an [existing storage VM](#) enabled for both NFS and SMB protocols.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. In ONTAP System Manager, click **Storage > Volumes** and then click **Add**.
 - a. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

1. Click **More Options** and select **Share via NFS**.

The default setting grants full access to all users. You can add more restrictive rules to the export policy later.

2. Select **Share via SMB/CIFS**.

The share is created with a default Access Control List (ACL) set to "Full Control" for the **Everyone** group. You can add restrictions to the ACL later.

3. On a Linux client, do the following to verify that the export is accessible.
 - a. Create and mount the volume using the network interface of the storage VM.
 - b. On the newly mounted volume, create a test file, write text to it, and then delete the file.
4. On a Windows client, do the following to verify that the share is accessible.
 - a. In Windows Explorer, map a drive to the share in the following format:
`__SMB_Server_Name__Share_Name__`
 - b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the volume's export policy](#), [restrict client access with the share ACL](#), and set any desired ownership and permissions on the exported and shared volume.

Secure client access with Kerberos

Enable Kerberos to secure storage access for NAS clients.

This procedure configures Kerberos on an existing storage VM enabled for [NFS](#) or [SMB](#).

Before beginning you should have configured DNS, NTP, and [LDAP](#) on the storage system.



Steps

1. At the ONTAP command line, set UNIX permissions for the storage VM root volume.

- Display the relevant permissions on the storage VM root volume: `volume show -volume root_vol_name-fields user,group,unix-permissions`

The root volume of the storage VM must have the following configuration:

Name...	Setting...
UID	root or ID 0
GID	root or ID 0
UNIX permissions	755

- If these values are not shown, use the `volume modify` command to update them.

2. Set user permissions for the storage VM root volume.

- Display the local UNIX users: `vserver services name-service unix-user show -vserver vserver_name`

The storage VM should have the following UNIX users configured:

User name	User ID	Primary group ID
nfs	500	0
root	0	0

Note: The NFS user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user; see step 5.

- If these values are not shown, use the `vserver services name-service unix-user modify` command to update them.

3. Set group permissions for the storage VM root volume.

- Display the local UNIX groups: `vserver services name-service unix-group show -vserver vserver_name`

The storage VM should have the following UNIX groups configured:

Group name	Group ID
daemon	1
root	0

- If these values are not shown, use the `vserver services name-service unix-group modify` command to update them.

4. Switch to System Manager to configure Kerberos

5. In ONTAP System Manager, click **Storage > Storage VMs** and select the storage VM.

6. Click **Settings**.

7. Click → under Kerberos.

8. Click **Add** under Kerberos Realm, and complete the following sections:

- Add Kerberos Realm
 - Enter configuration details depending on KDC vendor.
 - Add Network Interface to Realm
 - Click **Add** and select a network interface.
9. If desired, add mappings from Kerberos principal names to local user names.
- a. Click **Storage > Storage VMs** and select the storage VM.
 - b. Click **Settings**, and then click → under **Name Mapping**.
 - c. Under **Kerberos to UNIX**, add patterns and replacements using regular expressions.

Provide client access with name services

Enable ONTAP to look up host, user, group, or netgroup information using LDAP or NIS to authenticate NAS clients.

This procedure creates or modifies LDAP or NIS configurations on an existing storage VM enabled for [NFS](#) or [SMB](#).

For LDAP configurations, you should have the LDAP configuration details required in your environment and you should be using a default ONTAP LDAP schema.

Steps

1. Configure the required service: click **Storage > Storage VMs**.
2. Select the storage VM, click **Settings**, and then click  for LDAP or NIS.
3. Include any changes in the name services switch: click  under Name Services Switch.

Provision NAS storage for large file systems using FlexGroup volumes

A FlexGroup volume is a scalable NAS container that provides high performance along with automatic load distribution. FlexGroup volumes provide massive capacity (in petabytes), which considerably exceeds the FlexVol volume limits, without adding any management overhead.

Starting in System Manager 9.9.1, SnapMirror fanout relationships of 2 or more FlexGroup volumes are supported, with a maximum of 8 fanout legs. System Manager does not support SnapMirror cascading FlexGroup volume relationships.

ONTAP automatically selects the local tiers required for creating the FlexGroup volume.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

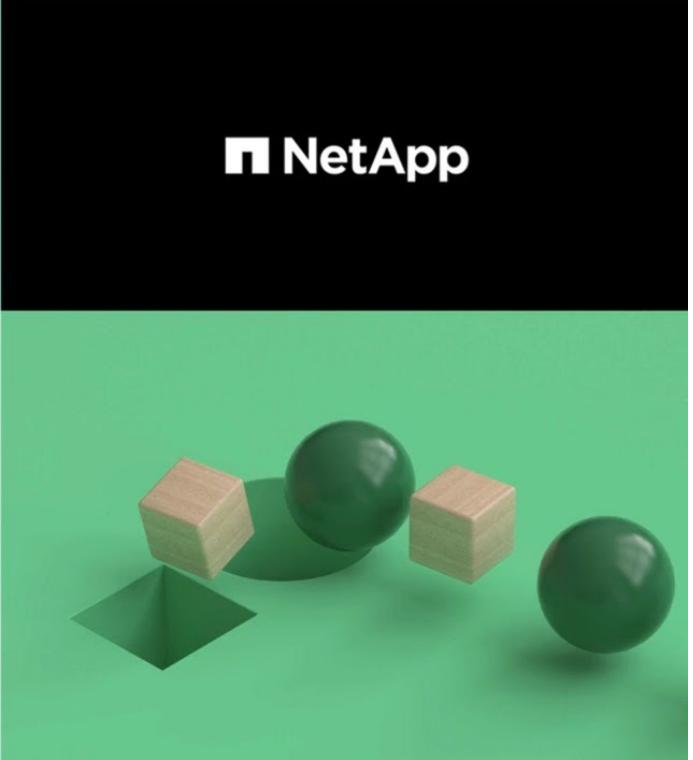
1. Click **Storage > Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Distribute volume data across the cluster**.
 - a. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

NetApp FlexGroup Volumes

Create and Manage a FlexGroup Volume

Tech Clip

© 2020 NetApp, Inc. All rights reserved.

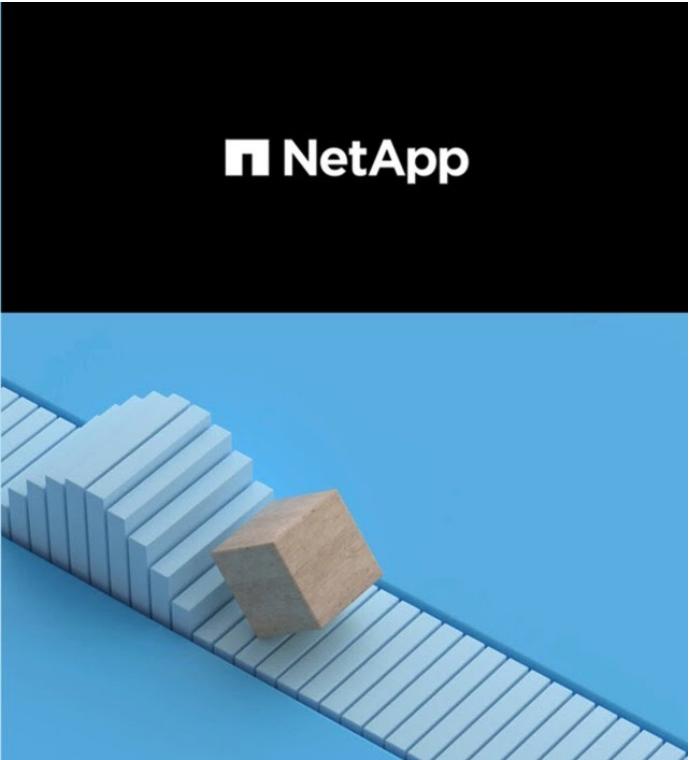


NetApp FlexGroup Volumes

Do More with Less

Use Case

© 2020 NetApp, Inc. All rights reserved.



Manage directories and files

Expand the System Manager volume display to view and delete directories and files.

Beginning in ONTAP 9.9.1, directories are deleted with low-latency fast directory delete functionality.

For more information about viewing file systems in ONTAP 9.9.1 and later, see [File System Analytics overview](#).

Step

1. Click **Storage > Volumes**. Then expand a volume to view its contents.

Monitor volume usage with ONTAP File System Analytics

File System Analytics overview

File System Analytics is a framework for collecting and displaying data about the contents of a FlexGroup or FlexVol volume.

File system analytics presents detailed information at each level of the volume's file system hierarchy, allowing you to:

- Assess capacity usage and trends
- Monitor file and directory counts
- Evaluate file activity and history
- Take corrective action based on displays (beginning with ONTAP 9.9.1)

In ONTAP 9.8 and later, file system analytics can be displayed using ONTAP System Manager. You can also use ONTAP REST APIs to access the data programmatically.

NOTE:

* Enabling file system analytics is expected to have a performance impact. Do not enable analytics if maximal performance is required in your environment. You can also disable analytics if your testing shows that the performance impact is unacceptable. When you disable analytics, previously collected data is no longer displayed for that volume.

* If you have enabled file system analytics on volumes whose containing SVM is in a protection relationship, the analytics data is not replicated to the destination SVM. If the source SVM must be resynchronized in a recovery operation, you must manually reenable analytics on desired volumes after recovery.

* Beginning with ONTAP 9.9.1, file system analytics is available for volumes transitioned from 7-mode systems. Nonetheless, because file system analytics can consume storage space, it should not be run on transitioned volumes that are close to maximum capacity.

File system analytics is not available for the following volume types:

- SnapMirror destination volumes
- SnapLock volumes
- Volumes containing LUNs
- Volumes used only to hold SMB/CIFS audit logs
- Node root volumes (/mroot)

Enable File System Analytics

To collect and display usage data, you must enable file system analytics. You can do so using System Manager, the ONTAP CLI, or REST APIs.

You can enable file system analytics when you create a new volume, or when you upgrade a system with volumes to ONTAP 9.8 or later. After upgrading, be sure that all upgrade processes have completed before enabling analytics.

Depending on the size and contents of the volume, enabling analytics might take some time while ONTAP processes existing data in the volume. System Manager displays progress and presents analytics data when complete. If you need more precise information about initialization progress, you can use the ONTAP CLI command `volume analytics show`.

Steps

1. Click **Storage > Volumes**, then select the desired volume.
2. Click **Explorer**, then click **Enable Analytics** or **Disable Analytics**.

View file system activity

After File System Analytics is enabled, by default, you can view the root directory contents of a selected volume sorted by the space used in each subtree.

Clicking on any file system object allows you to browse the file system and to display detailed information about each object in a directory. Information about directories can also be displayed graphically. Over time, historical data is displayed for each subtree. Space used is not sorted if there are more than 3000 directories.

The file system analytics **Explorer** screen consists of three areas:

- Tree view of directories and subdirectories; expandable list showing name, size, modify history, and access history.
- Files; showing name, size, and accessed time for the object selected in the directory list.
- Active and inactive data comparison for the object selected in the directory list.

Beginning with ONTAP 9.9.1, you can customize the range to be reported. The default is one year. Based on these customizations, you can take corrective actions, such as moving volumes and modifying the tiering policy.

Accessed time is shown by default. However, if the volume default has been altered from the CLI, by setting the `-atime-update` option to `false` with the `volume modify` command, only last modified time is shown. For example:

- The tree view will not display the **access history**.
- The files view will be altered.
- The active/inactive data view will be based on modified time (`mtime`).

Using these displays, you can examine the following:

- File system locations consuming the most space
- Detailed information about a directory tree, including file and subdirectory count within directories and

subdirectories

- File system locations that contain old data (for example, scratch, temp, or log trees)

Keep the following points in mind when interpreting file system analytics output:

- File system analytics show where and when your data is in use, not how much data is being processed. For example, large space consumption by recently accessed or modified files does not necessarily indicate high system processing loads.
- The way that the **Volume Explorer** tab calculates space consumption for file system analytics might differ from other tools. In particular, there could be significant differences compared to the consumption reported in the **Volume Overview** if the volume has storage efficiency features enabled. This is because the **Volume Explorer** tab does not include efficiency savings.
- Due to space limitations in the directory display, it is not possible to view a directory depth greater than 8 levels in the *List View*. To view directories more than 8 levels deep, you must switch to *Graphical View*, locate the desired directory, then switch back to *List View*. This will allow additional screen space in the display.

Step

1. Click **Storage > Volumes**, select the desired volume, then click **Explorer**.

Take corrective action based on analytics

Beginning with ONTAP 9.9.1, you can take corrective actions directly from File System Analytics displays based on current data and desired outcomes.

When analytics are enabled, you can take the following actions:

- delete directories and files

In the Explorer display, you can select directories or individual files to delete. Directories are deleted with low-latency fast directory delete functionality. (Fast directory delete is also available beginning in ONTAP 9.9.1 without analytics enabled.)

- assign media cost in storage tiers to compare costs of inactive data storage locations

Media cost is a value that you assign based on your evaluation of storage costs, represented as your choice of currency per GB. When set, ONTAP System Manager uses the assigned media cost to project estimated savings when you move volumes.

The media cost you set is not persistent; it can only be set for a single browser session.

- move volumes to reduce storage costs

Based on analytics displays and media cost comparisons, you can move volumes to less expensive storage in local tiers.

Only one volume at a time can be compared and moved.

Table 1. Steps

To perform this action...	Take these steps...
Delete directories or files	<p>1. Click Storage > Volumes, then click Explorer.</p> <p>When you hover over a file or folder, the option to delete appears. You can only delete one object at a time.</p> <p>Note When directories and files are deleted, the new storage capacity values are not displayed immediately.</p>
Enable media cost comparison	<p>1. Click Storage > Tiers, then click Set Media Cost in the desired local tier (aggregate) tiles.</p> <p>Be sure to select active and inactive tiers to enable comparison.</p> <p>2. Enter a currency type and amount.</p> <p>When you enter or change the media cost, the change is made in all media types.</p>
Move volumes to a less expensive tier	<p>1. After enabling media cost display, click Storage > Tiers, then click Volumes.</p> <p>2. To compare destination options for a volume, click  for the volume, then click Move.</p> <p>3. In the Select Destination Local Tier display, select destination tiers to display the estimated cost difference.</p> <p>4. After comparing options, select the desired tier and click Move.</p>

Monitor NFS active clients

Beginning with ONTAP 9.8, System Manager shows which NFS client connections are active when NFS is licensed on a cluster.

This allows you to quickly verify which NFS clients are actively connect to a storage VM, which are connected but idle, and which are disconnected.

For each NFS client IP address, the **NFS Clients** display shows:

- * Time of last access
- * Network interface IP address
- * NFS connection version
- * Storage VM name

In addition, a list of NFS clients active in the last 48 hours is also shown in the **Storage>Volumes** display and

a count of NFS clients is included in the **Dashboard** display.

Step

1. Display NFS client activity: Click **Hosts > NFS Clients**.

Improve performance for multiple clients with FlexCache

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes are ideal for read-intensive workloads, especially where clients need to access the same data repeatedly.

Learn how ONTAP FlexCache can reduce WAN latency and read times for global data.

The image shows a promotional graphic for ONTAP FlexCache. On the left, a light blue background features the text "ONTAP FlexCache" and "Data Access Where You Need It". Below this, the word "Use Case" is displayed in large, bold, blue letters. At the bottom left, there is a small copyright notice: "© 2020 NetApp, Inc. All rights reserved." On the right, a dark blue vertical bar contains the NetApp logo. The central visual is a 3D rendering of a wooden cube resting on a ramp made of blue rectangular blocks, symbolizing performance and speed.

Learn about the performance benefits of ONTAP FlexCache!

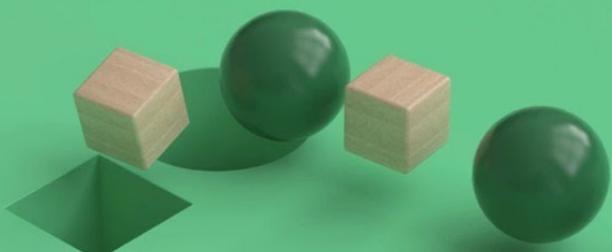
ONTAP FlexCache

Data Access Where You Need It

Tech Clip

© 2020 NetApp, Inc. All rights reserved.

NetApp



i Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. Click **Storage > Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Add as cache for a remote volume**.
 - a. If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then, under **Storage and Optimization** select **Performance Service Level**.

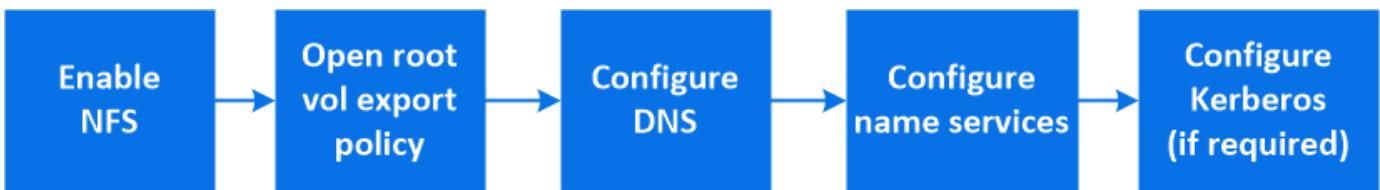
For any new data requests, the FlexCache volume requests the data from the remote volume and stores it. All the subsequent read requests for the data are then served directly from the FlexCache volume.

Enable NAS storage

Enable NAS storage for Linux servers using NFS

Modify storage VMs to enable NFS servers for serving data to Linux clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



Steps

1. Enable NFS on an existing VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click under **NFS**.
2. Open the export policy of the storage VM root volume:
 - a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name_root*), and then click on the policy that is displayed under **Export Policy**.
 - b. Click **Add** to add a rule.
 - Client specification = **0.0.0.0/0**
 - Access protocols = **NFS**
 - Access details = **UNIX Read-Only**
3. Configure DNS for host-name resolution: click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click under **DNS**.
4. Configure name services as required.
 - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click for LDAP or NIS.
 - b. Include any changes in the name services switch file: click in the Name Services Switch tile.
5. Configure Kerberos if required:
 - a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
 - b. Click in the Kerberos tile and then click **Add**.

Enable NAS storage for Windows servers using SMB/CIFS

Modify storage VMs to enable SMB servers for serving data to Windows clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



Steps

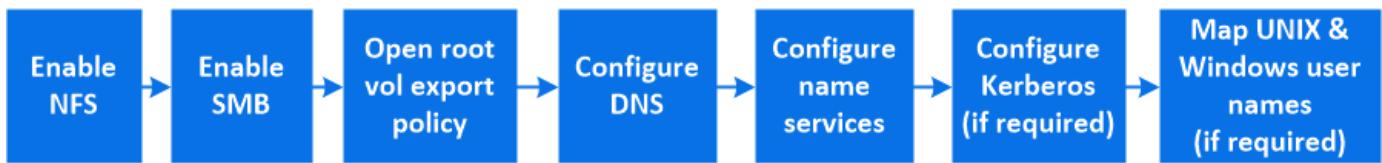
1. Enable SMB/CIFS on an existing VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click under **SMB/CIFS**.
2. Open the export policy of the storage VM root volume:
 - a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name_root*), and then click on the policy that is displayed under **Export Policy**.

- b. Click **Add** to add a rule.
 - Client specification = **0.0.0.0/0**
 - Access protocols = SMB/CIFS
 - Access details = NTFS Read-Only
3. Configure DNS for host-name resolution:
 - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click under **DNS**.
 - b. Switch to the DNS server and map the SMB server.
 - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
 - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
4. Configure name services as required
 - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click under **LDAP or NIS**.
 - b. Include any changes in the name services switch file: click under **Name Services Switch**.
5. Configure Kerberos if required:
 - a. Click **Storage > Storage VMs**, select the storage VM, and then click **Settings**.
 - b. Click under **Kerberos** and then click **Add**.

Enable NAS storage for both Windows and Linux using both NFS and SMB/CIFS

Modify storage VMs to enable NFS and SMB servers to serve data to Linux and Windows clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



Steps

1. Enable NFS on an existing VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click under **NFS**.
2. Enable SMB/CIFS on an existing VM: click under **SMB/CIFS**.
3. Open the export policy of the storage VM root volume:
 - a. Click **Storage > Volumes**, select the root volume of the storage VM (which by default is *volume-name_root*), and then click on the policy that is displayed under **Export Policy**.
 - b. Click **Add** to add a rule.
 - Client specification = **0.0.0.0/0**
 - Access protocols = NFS
 - Access details = NFS Read-Only

4. Configure DNS for host-name resolution:
 - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
 - b. When DNS configuration is complete, switch to the DNS server and map the SMB server.
 - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
 - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
5. Configure name services as required:
 - a. Click **Storage > Storage VMs**, select the storage VM, click **Settings**, and then click  for LDAP or NIS.
 - b. Include any changes in the name services switch file: click  under **Name Services Switch**.
6. Configure Kerberos if required: click  in the Kerberos tile and then click **Add**.
7. Map UNIX and Windows user names if required: click  under **Name Mapping** and then click **Add**.

You should use this procedure only if your site has Windows and UNIX user accounts that do not map implicitly, which is when the lowercase version of each Windows user name matches the UNIX user name. This procedure can be done using LDAP, NIS, or local users. If you have two sets of users that do not match, you should configure name mapping.

Provision object storage

The topics in this section show you how to configure and manage S3 object storage services with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage S3 object storage services, see this content:

- [S3 Configuration Power Guide](#)
- [Managing Storage Tiers By Using FabricPool](#)

ONTAP S3 overview for System Manager

Beginning with ONTAP 9.8, you can enable an ONTAP Simple Storage Service (S3) object storage server in an ONTAP cluster.

System Manager supports two on-premises use case scenarios for serving S3 object storage:

- FabricPool tier to a bucket on local cluster (tier to a local bucket) or remote cluster (cloud tier).
- S3 client app access to a bucket on the local cluster or a remote cluster.

For more information about tiering, see [Cloud overview](#).



ONTAP S3 is appropriate if you want S3 capabilities on existing clusters without additional hardware and management. For deployments larger than 300TB, NetApp StorageGRID software continues to be the NetApp flagship solution for object storage. For more information, see the [StorageGRID documentation](#).

When you create an S3 bucket using System Manager, ONTAP configures a default performance service level that is the highest available on your system. For example, on an AFF system, the default setting would be **Extreme**. Performance service levels are predefined adaptive Quality of Service (QoS) policy groups. Instead of one of the default service levels, you can specify a custom QoS policy group or no policy group.

Predefined adaptive QoS policy groups are:

- **Extreme**: Used for applications that expect the lowest latency and highest performance.
- **Performance**: Used for applications with modest performance needs and latency.
- **Value**: Used for applications for which throughput and capacity are more important than latency.
- **Custom**: Specify a custom QoS policy or no QoS policy.

If you select **Use for tiering**, no performance service levels are selected, and the system tries to select low-cost media with optimal performance for the tiered data.

See also: [Using adaptive QoS policy groups](#).

ONTAP tries to provision this bucket on local tiers that have the most appropriate disks, satisfying the chosen service level. However, if you need to specify which disks to include in the bucket, consider configuring S3 object storage from the CLI by specifying the local tiers (aggregate). If you configure the S3 server from the CLI, you can still manage it with System Manager if desired. For more information, see [S3 Configuration Power Guide](#).

Enable an S3 server on a storage

Add an S3 server to a new or existing storage VM for serving content to S3 clients.

An S3 server can coexist in a storage VM with other protocol servers, or you can create a new storage VM to isolate the namespace and workload.

Before you begin

You should be prepared to enter an S3 server name (FQDN) and IP addresses for interface role Data.

If you are using an external-CA signed certificate, you will be prompted to enter it during this procedure; you also have the option to use a system-generated certificate.

Steps

1. Enable S3 on a storage VM.

- a. Add a new storage VM: click **Storage > Storage VMs**, then click **Add**.

If this is a new system with no existing storage VMs: click **Dashboard > Configure Protocols**.

If you are adding an S3 server to an existing storage VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **S3**.

- b. Click **Enable S3**, then enter the S3 Server Name.

This will be the Fully Qualified Domain Name (FQDN) that clients will use.

- c. Select the certificate type.

Whether you select system-generated certificate or one of your own, it will be required for client access.

- d. Enter the network interfaces.

2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.

- The secret key will not be displayed again.

- If you need the certificate information again: click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

Provision buckets

Add an S3 bucket for the new S3 object store or add additional buckets to an existing object store.

For remote client access, you must configure buckets in an S3-enabled storage VM. If you create a bucket in a storage VM that is not S3-enabled, it will only be available for local tiering.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

Steps

1. Add a new bucket on an S3-enabled storage VM.
 - a. Click **Storage > Buckets**, then click **Add**.
 - b. Enter a name, select the storage VM, and enter a size.
 - If you click **Save** at this point, a bucket is created with these default settings:
 - No users are granted access to the bucket unless any group policies are already in effect.
2. On S3 client apps – another ONTAP system or an external 3rd-party app – verify access to the new bucket by entering the following:
 - The S3 server CA certificate.
 - The user's access key and secret key.
 - The S3 server FQDN name and bucket name.



You should not use the S3 root user to manage ONTAP object storage and share its permissions, because it has unlimited access to the object store. Instead, create a user or group with administrative privileges that you assign.

- A Quality of Service (performance) level that is the highest available for your system.
- You can click **More Options** to configure user permissions and performance level when you configure the bucket, or you can modify these settings later.
 - You must have already created user and groups before using **More Options** to configure their permissions.
 - If you intend to use the S3 object store for FabricPool tiering, consider selecting **Use for tiering** (use low-cost media with optimal performance for the tiered data) rather than a performance service level.

Add S3 users and groups

Edit the storage VM to add users, and to add users to groups.

Steps

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click under S3.
2. Add a user: click **Users**, then click **Add**.
 - a. Enter a name and click **Save**.
 - b. Be sure to save the access key and secret key, they will be required for access from S3 clients.
3. If desired, add a group: click **Groups**, then click **Add**.
 - a. Enter a group name and select from a list of users.
 - b. You can select an existing group policy or add one now, or you can add a policy later.

Manage user access to buckets

Edit the bucket to modify the list users with access to the bucket and specify their permissions.

User and group permissions can be granted when the bucket is created or as needed later. You can also

modify the bucket capacity and QoS policy group assignment.

You must have already created users or groups before granting permissions.

In ONTAP 9.9.1 and later releases, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

Steps

1. Edit the bucket: click **Storage > Buckets**, click the desired bucket, and then click **Edit**.

When adding or modifying permissions, you can specify the following parameters:

- Principal: the user or group to whom access is granted.
- Effect: allows or denies access to a user or group.
- Actions: permissible actions in the bucket for a given user or group.
- Resources: paths and names of objects within the bucket for which access is granted or denied.

The defaults **bucketname** and **bucketname/*** grant access to all objects in the bucket. You can also grant access to single objects; for example, **bucketname/*_readme.txt**.

- Conditions (optional): expressions that are evaluated when access is attempted. For example, you can specify a list of IP addresses for which access will be allowed or denied.

Manage user access to S3-enabled storage VMs

Edit the storage VM to add a policy that controls user and group access permissions to multiple buckets.

You can add a group policy to manage access to one or more buckets in an S3-enabled storage VM, rather than managing access permissions for individual buckets. Doing so simplifies management when buckets are added or when access needs change.

You must have already created users and at least one group before granting permissions in a policy.

In ONTAP 9.9.1 and later releases, if you plan to support AWS client object tagging functionality with the ONTAP S3 server, the actions `GetObjectTagging`, `PutObjectTagging`, and `DeleteObjectTagging` need to be allowed using the bucket or group policies.

Steps

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.
2. Add a user: click **Policies**, then click **Add**.
 - a. Enter a policy name and select from a list of groups.
 - b. Select an existing default policy or add a new one.

When adding or modifying a group policy, you can specify the following parameters:

- Group: the groups to whom access is granted.
- Effect: allows or denies access to one or more groups.
- Actions: permissible actions in one or more buckets for a given group.

- Resources: paths and names of objects within one or more buckets for which access is granted or denied.

For example:

- * grants access to all buckets in the storage VM.
- **bucketname** and **bucketname/*** grant access to all objects in a specific bucket.
- **bucketname/readme.txt** grants access to an object in a specific bucket.

c. If desired, add statements to existing policies.

Manage resources using quotas

The topics in this section show you how to configure and manage usage quotas with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage usage quotas, see this content:

- [Logical Storage Management Guide](#)

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to configure and manage usage quotas, see the content for your ONTAP release:

- [Cluster management using System Manager 9.6 and 9.7](#)
- [Cluster management using System Manager 9.5](#)
- [Cluster management using System Manager 9.3 and 9.4](#)
- [Cluster management using System Manager 9.2 and earlier](#)

Quota overview

Quotas provide a way to restrict or track the disk space and number of files used by a user, group, or qtree. Quotas are applied to a specific volume or qtree.

You can use quotas to track and limit resource usage in volumes and provide notification when resource usage reaches specific levels.

Quotas can be soft or hard. Soft quotas cause ONTAP to send a notification when specified limits are exceeded, and hard quotas prevent a write operation from succeeding when specified limits are exceeded.

Set quotas to limit resource use

Add quotas to limit the amount of disk space the quota target can use.

You can set a hard limit and a soft limit for a quota.

Hard quotas impose a hard limit on system resources; any operation that would result in exceeding the limit fails. Soft quotas send a warning message when resource usage reaches a certain level, but they do not affect data access operations, so you can take appropriate action before the quota is exceeded.

Steps

1. Click **Storage > Quotas**.
2. Click **Add**.

Maximize security

The topics in this section show you how to manage cluster security with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to manage cluster security, see this content:

- [Administrator Authentication and RBAC Power Guide](#)
- [Antivirus Configuration Guide](#)
- [NetApp Encryption Power Guide](#)

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to manage cluster security, see the content for your ONTAP release:

- [Cluster management using System Manager 9.6 and 9.7](#)
- [Cluster management using System Manager 9.5](#)
- [Cluster management using System Manager 9.3 and 9.4](#)
- [Cluster management using System Manager 9.2 and earlier](#)

Security overview for System Manager

With System Manager, you use ONTAP standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest and for WORM storage.

Client authentication and authorization

ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

Administrator authentication and RBAC

Administrators use local or remote login accounts to authenticate themselves to the cluster and storage VM. Role-Based Access Control (RBAC) determines the commands to which an administrator has access.

Virus scanning

You can use integrated antivirus functionality on the storage system to protect data from being compromised by viruses or other malicious code. ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

Encryption

ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

WORM storage

SnapLock is a high-performance compliance solution for organizations that use *write once, read many* (WORM) storage to retain critical files in unmodified form for regulatory and governance purposes.

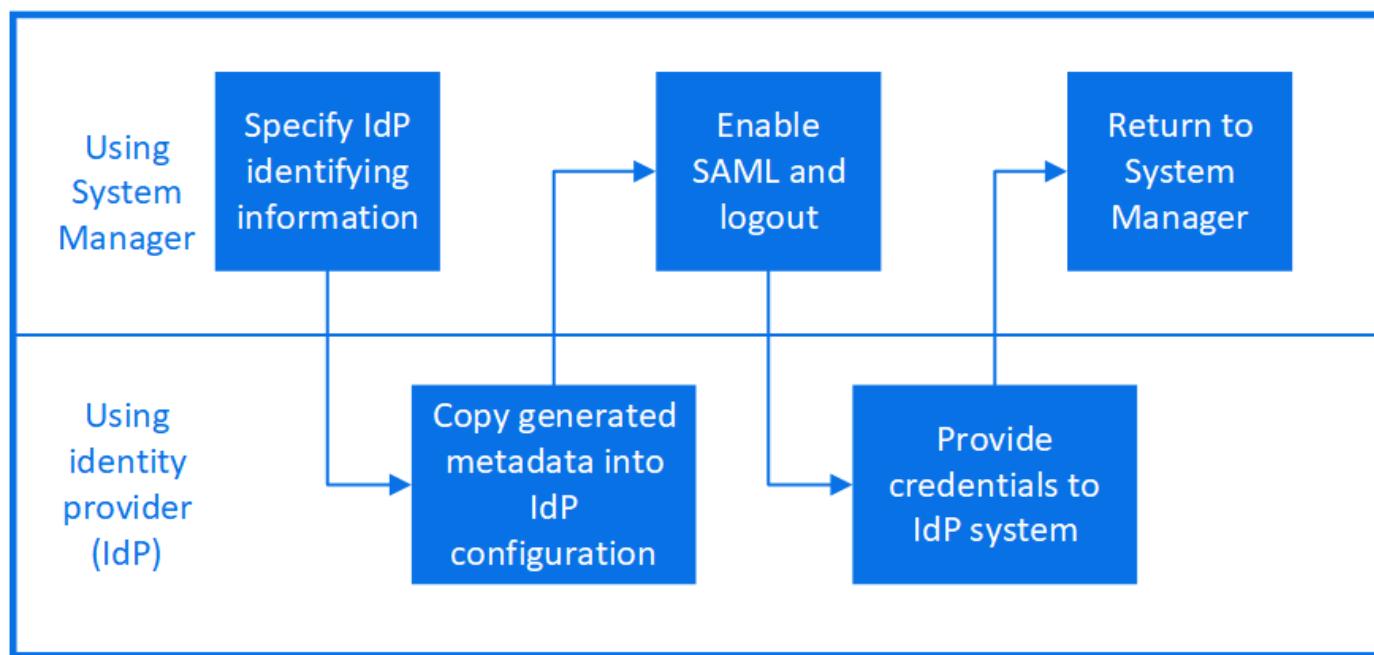
Set up multifactor authentication

Security Assertion Markup Language (SAML) authentication allows users to log in to an application by using a secure identity provider (IdP).

In System Manager, in addition to standard ONTAP authentication, SAML-based authentication is provided as an option for multifactor authentication.

Security Assertion Markup Language (SAML) is an XML-based framework for authentication and authorization between two entities: a service provider and an identity provider.

Enable SAML authentication



To enable SAML authentication, perform the following steps:

Steps

1. Click **Cluster > Settings**.
2. Next to **SAML Authentication**, click .
3. Ensure there is a check in the **Enable SAML Authentication** checkbox.
4. Enter the URL of the IdP URI (including "https://").
5. Modify the host system address, if needed.
6. Ensure the correct certificate is being used:
 - If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.

- If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.
7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.
 8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata.
 9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.
 10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.
 11. In the IdP system, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

Disable SAML authentication

To disable SAML authentication, perform the following steps:

Steps

1. Click **Cluster > Settings**.
2. Under **SAML Authentication**, click the **Enabled** toggle button.
3. *Optional:* You can also click  next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

Control administrator access

The role assigned to an administrator determines which functions the administrator can perform with System Manager. Predefined roles for cluster administrators and storage VM administrators are provided by System Manager. You assign the role when you create the administrator's account, or you can assign a different role later.

Depending on how you have enabled account access, you might need to perform any of the following:

- Associate a public key with a local account.
- Install a CA-signed server digital certificate.
- Configure AD, LDAP, or NIS access.

You can perform these tasks before or after enabling account access.

Assigning a role to an administrator

Assign a role to an administrator, as follows:

Steps

1. Click **Cluster > Settings**.
2. Click  next to **Users and Roles**.
3. Click  **Add** under **Users**.
4. Specify a user name, and select a role in the drop-down menu for **Role**.

5. Specify a login method and password for the user.

Changing an administrator's role

Change the role for an administrator, as follows:

Steps

1. Click **Cluster > Settings**.
2. Select the name of user whose role you want to change, then click the  that appears next to the user name.
3. Click **Edit**.
4. Select a role in the drop-down menu for **Role**.

Encrypt stored data using software-based encryption

Use volume encryption to ensure that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Volume encryption does not require special disks; it works with all HDDs and SSDs.

Volume encryption requires a key manager. You can configure the Onboard Key Manager using ONTAP System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

After the key manager is configured, new volumes are encrypted by default.

Steps

1. Click **Cluster > Settings**.
2. Under **Encryption**, click  to configure the Onboard Key Manager for the first time.
3. To encrypt existing volumes, click **Storage > Volumes**.
4. On the desired volume, click  and then click **Edit**.
5. Select **Enable encryption**.

Encrypt stored data using self-encrypting drives

Use disk encryption to ensure that all data in a local tier cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Disk encryption requires special self-encrypting HDDs or SSDs.

Disk encryption requires a key manager. You can configure the onboard key manager using ONTAP System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

If ONTAP detects self-encrypting disks, it prompts you to configure the onboard key manager when you create the local tier.

Steps

1. Under **Encryption**, click  to configure the onboard key manager.
2. If you see a message that disks need to be rekeyed, click , and then click **Rekey Disks**.

Diagnose and correct file access issues

Starting with ONTAP 9.8, you can trace file access permissions with System Manager to diagnose why clients cannot access files.

Steps

1. In ONTAP System Manager, select **Storage > Storage VMs**.
2. Select the storage VM on which you want to perform a trace.
3. Click  **More**.
4. Click **Trace File Access**.
5. Provide the user name and client IP address, then click **Start Tracing**.

The trace results are displayed in a table. The **Reasons** column provides the reason why a file could not be accessed.

6. Click  in the left column of the results table to view the file access permissions.

Protect data

The topics in this section show you how to configure and manage data protection with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage data protection, see this content:

- [Archive and Compliance Using SnapLock Technology Power Guide](#)
- [Cluster and SVM Peering Power Guide](#)
- [Data Protection Power Guide](#)
- [Data Protection Tape Backup and Recovery Guide](#)
- [NDMP Configuration Express Guide](#)
- [Replication between NetApp Element Software and ONTAP](#)

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to configure and manage data protection, see the content for your ONTAP release:

- [Cluster and SVM Peering Express Guide](#)
- [Volume Disaster Recovery Express Guide](#)
- [Volume Disaster Recovery Preparation Express Guide](#)
- [Volume Backup Using SnapVault Express Guide](#)
- [Volume Restore Using SnapVault Express Guide](#)
- [Cluster management using System Manager 9.6 and 9.7](#)
- [Cluster management using System Manager 9.5](#)
- [Cluster management using System Manager 9.3 and 9.4](#)
- [Cluster management using System Manager 9.2 and earlier](#)

Data protection overview

Protect your data by creating and managing Snapshot copies, mirrors, vaults, and mirror-and-vault relationships.

SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or mirror, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.

A *vault* is designed for disk-to-disk Snapshot copy replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a vault destination typically retains point-in-time Snapshot copies created over a much longer period.

Create custom data protection policies

You can create custom data protection policies in System Manager when the existing default protection policies are not appropriate for your needs.

Create custom protection policies on both the source and destination cluster.

Steps

1. Click Protection > Local Policy Settings.
2. Under **Protection Policies**, click .
3. In the **Protection Policies** pane, click  **Add**.
4. Complete the required fields.
5. Click **Save**.
6. Repeat these steps on the other cluster.

Configure Snapshot copies

You can create Snapshot copy policies to specify the maximum number of Snapshot copies that are automatically created and how frequently they are created. The policy specifies when to create Snapshot copies, how many copies to retain, and how to name them.

This procedure creates a Snapshot copy policy on the local cluster only.

Steps

1. Click **Protection > Overview > Local Policy Settings**.
2. Under **Snapshot Policies**, click , and then click  **Add**.
3. Type the policy name, select the policy scope, and under **Schedules**, click  **Add** to enter the schedule details.

Recover from Snapshot copies

You can recover a volume to an earlier point in time by restoring from a Snapshot copy.

This procedure restores a volume from a Snapshot copy.

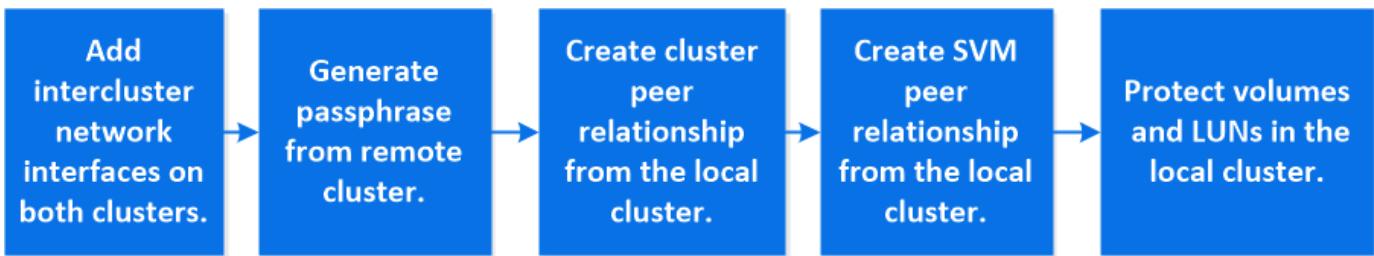
Steps

1. Click **Storage** and select a volume.
2. Under **Snapshot Copies**, click  next to the Snapshot copy you want to restore, and select **Restore**.

Prepare for mirroring and vaulting

You can protect your data by replicating it to a remote cluster for data backup and disaster recovery purposes.

Several default protection policies are available. You must have created your protection policies if you want to use custom policies.



Steps

1. In the local cluster, click **Protection > Overview**.
2. Expand **Intercluster Settings**. Click **Add Network Interfaces** and add intercluster network interfaces for the cluster.
Repeat this step on the remote cluster.
3. In the remote cluster, click **Protection > Overview**. Click **:** in the Cluster Peers section and click **Generate Passphrase**.
4. Copy the generated passphrase and paste it in the local cluster.
5. In the local cluster, under Cluster Peers, click **Peer Clusters** and peer the local and remote clusters.
6. Optionally, under Storage VM Peers, click **:** and then **Peer Storage VMs** to peer the storage VMs.
7. Click **Protect Volumes** to protect your volumes. To protect your LUNs, click **Storage > LUNs**, select a LUN to protect, and then click **Protect**.

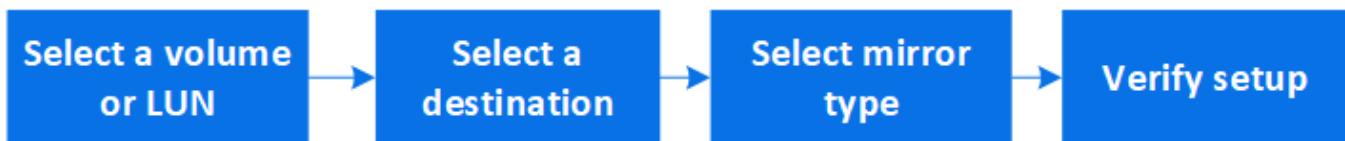
Select the protection policy based on the type of data protection you need.

8. To verify the volumes and LUNs are successfully protected from the local cluster, click **Storage > Volumes** or **Storage > LUNs** and, expand the volume/LUN view.

Configure mirrors and vaults

Create a mirror and vault of a volume to protect data in case of a disaster and to have multiple archived versions of data to which you can roll back. Only the combined mirror-and-vault policy is supported. You cannot specify separate mirror and vault policies.

This procedure creates a mirror-and-vault policy on a remote cluster. The source cluster and destination cluster use intercluster network interfaces for exchanging data. The procedure assumes the [intercluster network interfaces are created and the clusters containing the volumes are peered](#) (paired). You can also peer storage VMs for data protection; however, if storage VMs are not peered, but permissions are enabled, storage VMs are automatically peered when the protection relationship is created.



Steps

1. Select the volume or LUN to protect: click **Storage > Volumes** or **Storage > LUNs**, and then click the desired volume or LUN name.
2. Click **Protect**.

3. Select the destination cluster and storage VM.
4. The asynchronous policy is selected by default. To select a synchronous policy, click **More Options**.
5. Click **Protect**.
6. Click the **SnapMirror (Local or Remote)** tab for the selected volume or LUN to verify that protection is set up correctly.

Configure storage VM disaster recovery

You can create an storage VM disaster recovery (storage VM DR) relationship to replicate one storage VM configuration to another. In the event of a disaster at the primary site, you can quickly activate the destination storage VM.

Complete this procedure from the destination. If you need to create a new protection policy, for instance, when your source storage VM has CIFS configured, you should use System Manager to create the policy and select the **Copy source storage VM configuration** option in the **Add Protection Policy** window.

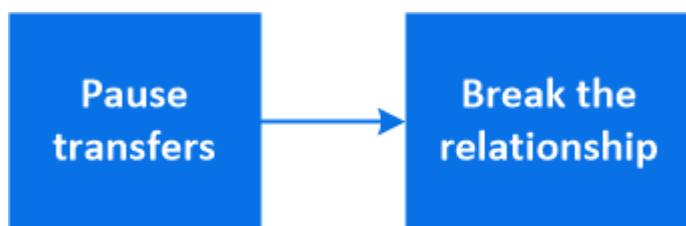
For details see [Create custom data protection policies](#).

Steps

1. On the destination cluster, click **Protection > Relationships**.
2. Under **Relationships**, click **Protect** and choose **Storage VMs (DR)**.
3. Select a protection policy. If you created a custom protection policy, select it, then choose the source cluster and storage VM you want to replicate. You can also create a new destination storage VM by entering a new storage VM name.
4. Click **Save**.

Serve data from a SnapMirror destination

To serve data from a mirror destination when a source becomes unavailable, stop scheduled transfers to the destination, and then break the SnapMirror relationship to make the destination writable.



Steps

1. Select the desired protection relationship: click **Protection > Relationships**, and then click the desired volume name.
2. Click **:**.
3. Stop scheduled transfers : click **Pause**.
4. Make the destination writable: click **Break**.
5. Go to the main **Relationships** page to verify that the relationship state displays as "broken off".

Next steps:

When the disabled source volume is available again, you should resynchronize the relationship to copy the current data to the original source volume. This process replaces the data on the original source volume.

Resynchronize a protection relationship

When your original source volume is available again after a disaster, you can resynchronize data from the destination volume and reestablish the protection relationship.

This procedure replaces the data in the original source volume in an asynchronous relationship so that you can start serving data from the original source volume again and resume the original protection relationship.

Steps

1. Click **Protection > Relationships** and then click the broken off relationship you want to resynchronize.
2. Click  and then select **Resync**.
3. Under **Relationships**, monitor the resynchronization progress by checking the relationship state. The state changes to "Mirrored" when resynchronization is complete.

Restore a volume from an earlier Snapshot copy

When data in a volume is lost or corrupted, you can roll back your data by restoring from an earlier Snapshot copy.

This procedure replaces the current data on the source volume with data from an earlier Snapshot copy version. You should perform this task on the destination cluster.

Steps

1. Click **Protection > Relationships**, and then click the source volume name.
2. Click  and then select **Restore**.
3. Under **Source**, the source volume is selected by default. Click **Other Volume** if you want to choose a different volume.
4. Under **Destination**, choose the Snapshot copy you want to restore.
5. If your source and destination are located on different clusters, on the remote cluster, click **Protection > Relationships** to monitor the restore progress.

Restore to a new volume

Starting in System Manager 9.8, you can restore backed up data on the destination volume to a volume other than the original source.

When you restore to a different volume, you can select an existing volume, or you can create a new volume.

Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click  and click **Restore**.

3. Under **Relationships**, monitor the restore progress by viewing **Transfer Status** for the relationship.

Reverse Resynchronizing a Protection Relationship

Starting in System Manager 9.8, you can perform a reverse resynchronization operation to delete an existing protection relationship and reverse the functions of the source and destination volumes. Then you use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

When you perform a reverse resynch operation, any data on the source volume that is newer than the data in the common Snapshot copy is deleted.

Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click  and click **Reverse Resync**.
3. Under **Relationships**, monitor the reverse resynchronization progress by viewing **Transfer Status** for the relationship.

Reactivate a source storage VM

Starting in System Manager 9.8, you can reactivate a source storage VM after a disaster. Reactivating the source storage VM stops the destination storage VM, and it reenables replication from the source to the destination.

Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click  and click **Reactivate Source Storage VM**.
3. Under **Relationships**, monitor the source reactivation progress by viewing **Transfer Status** for the protection relationship.

Resynchronize a destination storage VM

You can resynchronize the data and configuration details from the source SVM to the destination SVM in a broken protection relationship and reestablish the relationship.

You perform the resync operation only from the destination of the original relationship. The resync deletes any data in the destination storage VM that is newer than the data in the source storage VM.

Steps

1. Select the desired protection relationship: click **Protection > Relationships**.
2. Click  and click **Resync**.
3. Under **Relationships**, monitor the resynchronization progress by viewing **Transfer Status** for the relationship.

Back up to the cloud

Starting in System Manager 9.9.1, you can use System Manager to back up your data to the cloud and to restore your data from cloud storage to a different volume. You can use either StorageGRID or ONTAP S3 as your cloud object store.

Before you use SnapMirror Cloud with System Manager, you should generate a SnapMirror Cloud API license key on the NetApp Support Site: [Generate SnapMirror Cloud API license key](#)

Add a cloud object store

Before you configure SnapMirror Cloud backups, you should add a StorageGRID or ONTAP S3 cloud object store.

Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Click  **Add**.

Back up using the default policy

You can quickly configure a SnapMirror Cloud backup for an existing volume using the default cloud protection policy, DailyBackup.

Steps

1. Click **Protection > Overview** and select **Back Up Volumes to Cloud**.
2. If this is your first time backing up to the cloud, enter your SnapMirror Cloud API license key in the license field as indicated.
3. Click **Authenticate and Continue**.
4. Select a source volume.
5. Select a cloud object store.
6. Click **Save**.

Create a custom cloud backup policy

If you do not want to use the default DailyBackup cloud policy for your SnapMirror Cloud backups, you can create your own policy.

Steps

1. Click **Protection > Overview > Local Policy Settings** and select **Protection Policies**.
2. Click **Add** and enter the new policy details.
3. In the **Policy Type** section, select **Back up to Cloud** to indicate that you are creating a cloud policy.
4. Click **Save**.

Create a backup from the Volumes page

You can use the System Manager **Volumes** page to when you want to select and create cloud backups for multiple volumes at one time or when you want to use a custom protection policy.

Steps

1. Click **Storage > Volumes**.
2. Select the volumes you want to back up to the cloud, and click **Protect**.
3. In the **Protect Volume** window, click **More Options**.
4. Select a policy.

You can select the default policy, DailyBackup, or a custom cloud policy you created.

5. Select a cloud object store.
6. Click **Save**.

Restore from the cloud

You can use System Manager to restore backed up data from cloud storage to a different volume on the source cluster.

Steps

1. Click **Storage > Volumes** and select the volume you want to restore.
2. Click  next to the source volume and select **Restore**.
3. Under **Source**, select a storage VM and then enter the name of the volume to which you want the data restored.
4. Under **Destination**, select the Snapshot copy you want to restore.
5. Click **Save**.

Delete a SnapMirror Cloud relationship

You can use System Manager to delete a cloud relationship.

Steps

1. Click **Storage > Volumes** and select the volume you want to delete.
2. Click  next to the source volume and select **Delete**.
3. Select **Delete the cloud object store endpoint (optional)** if you want to delete the cloud object store endpoint.
4. Click **Delete**.

Remove a cloud object store

You can use System Manager to remove a cloud object store if it is not part of a cloud backup relationship. When a cloud object store is part of a cloud backup relationship, it cannot be deleted.

Steps

1. Click **Protection > Overview > Cloud Object Stores**.
2. Select the object store you want to delete, click  and select **Delete**.

Extend to the cloud

The topics in this section show you how to configure and manage a cloud tier with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to configure and manage a cloud tier, see this content:

- [Managing Storage Tiers By Using FabricPool](#)
- [S3 Configuration Power Guide](#)

If you are using legacy OnCommand System Manager for ONTAP 9.5-9.7 releases to configure and manage a cloud tier, see the content for your ONTAP release:

- [Cluster management using System Manager 9.6 and 9.7](#)
- [Cluster management using System Manager 9.5](#)

Cloud overview

You can use FabricPool to automatically tier data depending on how frequently the data is accessed.

FabricPool is a hybrid storage solution that uses an all flash (all SSD) aggregate as the performance tier and an object store as the cloud tier. Using a FabricPool helps you reduce storage cost without compromising performance, efficiency, or protection.

The cloud tier can be located on NetApp StorageGRID or ONTAP S3 (beginning with ONTAP 9.8), or one of the following service providers:

- Alibaba cloud
- Amazon S3
- Google Cloud
- IBM cloud
- Microsoft Azure Blob Storage

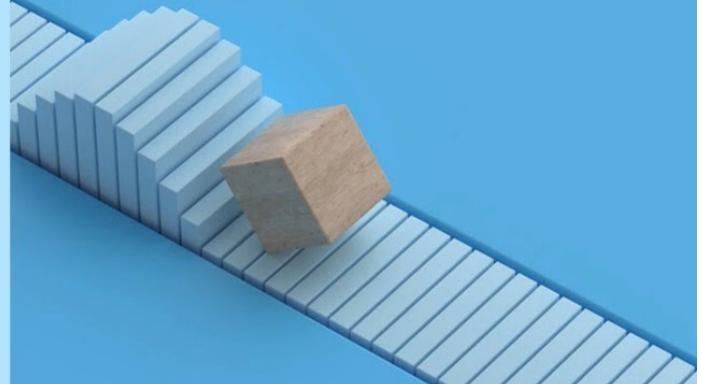
ONTAP FabricPool

Tier Data and Lower Costs

Use Case

© 2020 NetApp, Inc. All rights reserved.

 NetApp



Add a connection to the cloud

Starting with ONTAP 9.9.0, you can use System Manager to add a connection to the cloud.

You start by using NetApp Cloud Insights to configure a collector. During the configuration process, you copy a pairing code that is generated by Cloud Insights, and then you log on to a cluster using System Manager. There, you add a cloud connection using that pairing code. The rest of the process is completed in Cloud Insights.

Steps

1. In Cloud Insights, during the process to configure a collector, copy the generated pairing code.
2. Using System Manager 9.9.0 or later, log on to the cluster.
3. Go to **Cluster > Settings**.
4. In the Cloud Connections section, select **Add** to add a connection.
5. Enter a name for the connection, and paste the pairing code in the space provided.
6. Click **Add**.
7. Return to Cloud Insights to complete the configuration of the collector.



For additional information about using Cloud Insights, refer to [Cloud Insights Cloud Agent documentation](#).

Tier data to cloud

Storing data in tiers can enhance the efficiency of your storage system. You can manage

storage tiers by using FabricPool to store data in a tier, based on how frequently the data is accessed.

This procedure sets up an object store as the cloud tier for FabricPool. Keep in mind that once you attach to a local tier (aggr) the cloud tier cannot be unattached.

A FabricPool license is not required when using StorageGRID or ONTAP S3 as the cloud tier or when using Amazon S3, Google Cloud Storage, or Microsoft Azure Blob Storage as the cloud tier for Cloud Volumes for ONTAP. A FabricPool license is required for other cloud tier locations.

If you are tiering to ONTAP S3, there are additional requirements:

- * There must be an entry for the remote ONTAP S3 server's hostname in the DNS server configured for the admin storage VM, including the S3 server's FQDN name and the IP addresses on its network interfaces.

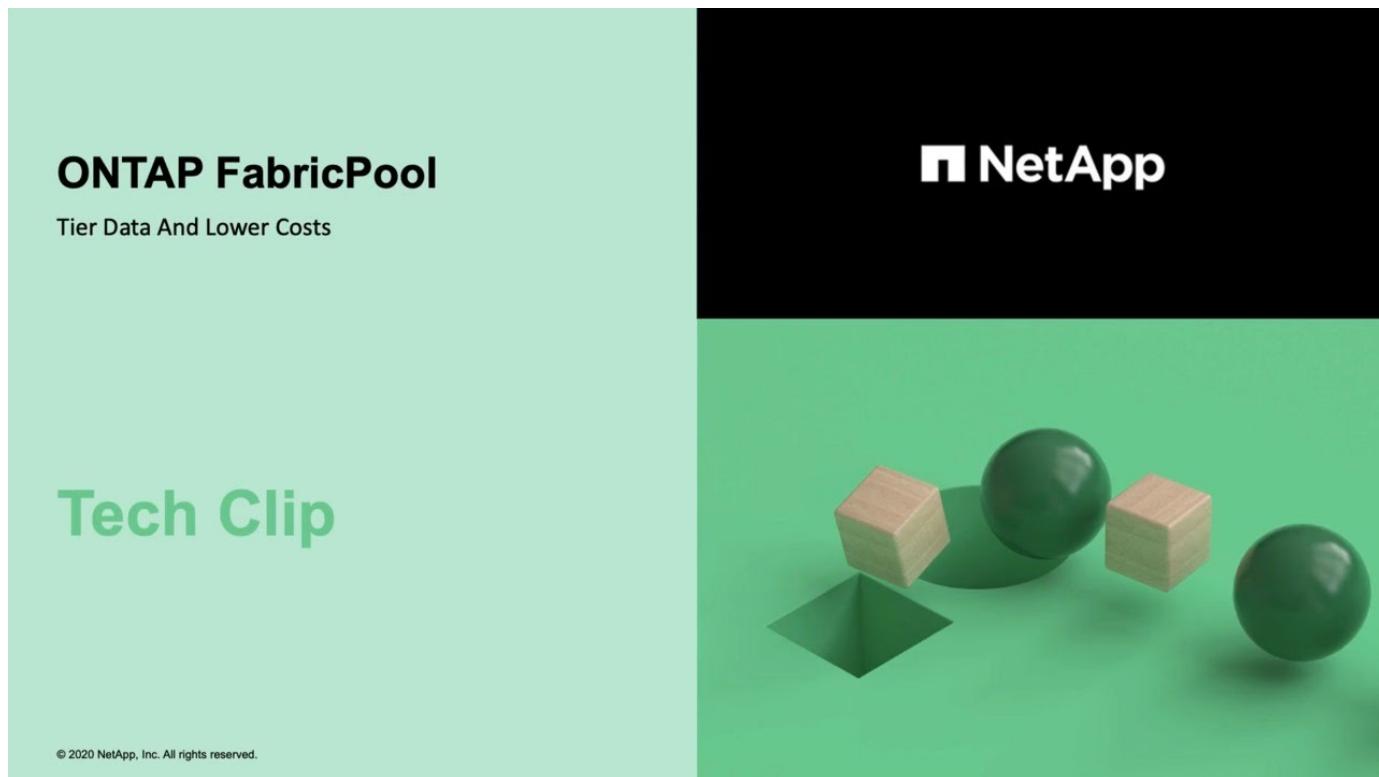
- * [Intercluster network interfaces](#) must be configured on both local and remote clusters, although cluster peering is not required.

You also have the option to create a volume tiering policy in System Manager.

Steps

1. Click **Storage > Tiers > Add Cloud Tier** and select the object store provider you want to use.
2. If you want to create a cloud mirror, click **Add as FabricPool Mirror**.

A FabricPool mirror provides a method for you to seamlessly replace a data store, and it helps to ensure that your data is available in the event of disaster.



Tier data to local bucket

Beginning with ONTAP 9.8, you can tier data to local object storage using ONTAP S3.

Tiering data to a local bucket provides a simple alternative to moving data to a different local tier. This procedure uses an existing bucket on the local cluster, or you can let ONTAP automatically create a new storage VM and a new bucket.

Keep in mind that once you attach to a local tier (aggr) the cloud tier cannot be unattached.

An S3 license is required for this workflow, which creates a new S3 server and new bucket, or uses existing ones. A FabricPool license is not required for this workflow.

Step

1. Tier data to a local bucket: click **Tiers**, select a tier, then click :
 - You have the option to create a new tier (ONTAP S3) or use an existing one.
 - You have the option to edit an existing volume tiering policy.

Create tags for tiering objects

Starting in ONTAP 9.8, you can create object tags to help you classify and sort tiering objects for easier data management. You can set tags only on FabricPool volumes attached to StorageGRID. These tags are retained during a volume move.

Steps

1. Navigate to **Storage > Tiers > Volumes**.
2. Locate the volume you want to tag and select **Click to enter tags**.

Enable inactive data reporting

Starting in ONTAP 9.8, you can enable inactive data reporting to show how much inactive data can be tiered to the cloud.

You can enable inactive data reporting on HDD aggregates.

Steps

1. Choose one of the following options:
 - When you have existing HDD aggregates, navigate to **Storage > Tiers** and click  for the aggregate on which you want to enable inactive data reporting.
 - When no cloud tiers are configured, navigate to **Dashboard** and click the **Enable inactive data reporting** link under **Capacity**.

Back up data using the Cloud Backup Service

Starting with ONTAP 9.9.1, you can use System Manager to back up data in the cloud using Cloud Backup Service.



Cloud Backup Service supports FlexVol read-write volumes and data-protection (DP) volumes. FlexGroup volumes and SnapLock volumes are not supported.

Before you begin

You should perform the following procedures to establish an account in Cloud Manager.

1. [Create an account in Cloud Manager](#).
2. [Create a connector in Cloud Manager](#) with one of the following cloud providers:
 - Microsoft Azure
 - Amazon Web Services (AWS)
 - Google Cloud Platform (GCP)
3. [Subscribe to Cloud Backup Service in Cloud Manager](#) (requires the appropriate license).
4. [Generate an access key and a secret key using Cloud Manager](#).

Register the cluster with Cloud Manager

You can register the cluster with Cloud Manager by using either Cloud Manager or System Manager.

Steps

1. In System Manager, go to **Protection Overview**.
2. Under **Cloud Backup Service**, provide the following details:
 - Client ID
 - Client secret key
3. Select **Register and Continue**.

Enable the Cloud Backup Service

After the cluster is registered with Cloud Manager, you can enable the Cloud Backup Service and initiate the first backup to the cloud.

Steps

1. On the **Enable Cloud Backup Service** page, provide the following details:
 - Protection policy (an existing or new policy)
 - Cluster IP space
2. Select the checkbox if you want to back up all volumes in the cluster.
3. Select **Enable**.
4. Depending on which Cloud provider you specified, you need to provide specific information, as follows:

For this cloud provider...	Enter the following data...
Azure	<ul style="list-style-type: none">• Azure Subscription ID• Resource group name (existing or new)• Region• IPspace

For this cloud provider...	Enter the following data...
AWS	<ul style="list-style-type: none"> • AWS Account ID • Access key • Secret key • Region • IPspace
Google Cloud Project (GCP)	<ul style="list-style-type: none"> • Google Cloud Project name • Google Cloud Access key • Google Cloud Secret key • Region • IPspace

Protect new volumes or LUNs on the cloud

When you create a new volume or LUN, you can establish a SnapMirror protection relationship that enables backing up to the cloud for the volume or LUN.

Before you begin

- You should have a SnapMirror license.
- The WORM feature should be disabled.
- Intercluster LIFs should be configured.
- NTP should be configured.
- Cluster must be running ONTAP 9.9.1.
- You cannot use the feature for the following cluster configurations:
 - The cluster cannot be in a MetroCluster environment.
 - SVM-DR is not supported.
 - FlexGroups cannot be backed up using the Cloud Backup Service.

Steps

1. When provisioning a volume or LUN, on the **Protection** page, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
2. Select **Enable Cloud Backup Service**.

Protect existing volumes or LUNs on the cloud

You can establish a SnapMirror protection relationship for existing volumes and LUNs.

Steps

1. Select an existing volume or LUN, and click **Protect**.
2. On the **Protect Volumes** page, specify "Backup using Cloud Backup Service" for the protection policy.

3. Click **Protect**.
4. On the **Protection** page, select the checkbox labeled **Enable SnapMirror (Local or Remote)**.
5. Select **Enable Cloud Backup Service**.

Restore data from backup files

You can perform backup management operations, such as restoring data, updating relationships, and deleting relationships, only with Cloud Manager. Refer to [Restoring data from backup files](#) for more information.

Manage the connection to the Cloud Backup Service

Starting with ONTAP 9.9.1, you can use System Manager to back up data in the cloud using the Cloud Backup Service. You can manage the connection to the Cloud Backup Service and view details about the number and capacity of the volumes that are backed up using the service.

Before you begin

You should establish an account in Cloud Manager. See [Back up data using the Cloud Backup Service](#) for details.

View the status of the connection to the Cloud Backup Service

You can view various details about the connection to the Cloud Backup Service.

Steps

1. Go to **Protection > Overview**.
2. In the **Cloud Backup Service** section, you can view the following details:
 - Status of the connection.
 - The cloud provider.
 - The cloud manager workspace.
 - The number of backed up volumes.
 - The cloud provider used capacity.
 - The cloud manager connector ID.

Modify the connection with the Cloud Backup Service

You can modify the connection to the Cloud Backup Service.

Steps

1. Go to **Protection > Overview**.
2. In the **Cloud Backup Service** section, click .
3. You can select any of the following modification procedures:
 - **Edit:** Allows you to change the protection policy and the IPspace.
 - **Disable:** Stops all further backup operations to the cloud for the cluster.
 - **Unlink:** Removes the management of backups to the cloud provider from ONTAP System Manager.

However, backups will continue, and they can be managed using Cloud Manager.

View cluster performance

The topics in this section show you how to manage cluster health and performance with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using Active IQ Unified Manager to manage cluster health and performance, see this content:

- [Performance Management Power Guide](#)
- [Performance Monitoring Express Guide](#)

If you are using the ONTAP CLI to manage cluster health and performance, see this content:

- [EMS Configuration Express Guide](#)
- [System Administration Reference](#)

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to manage cluster health and performance, see the content for your ONTAP release:

- [SNMP Configuration Express Guide](#)
- [Cluster management using System Manager 9.6 and 9.7](#)
- [Cluster management using System Manager 9.5](#)
- [Cluster management using System Manager 9.3 and 9.4](#)
- [Cluster management using System Manager 9.2 and earlier](#)

Cluster performance overview with System Manager

The System Manager Dashboard provides the following performance information:

- **Health:** You can monitor the health of a cluster. Alerts are shown when problems arise.
- **Capacity:** System Manager shows you the available capacity on the cluster.
- **Performance:** You can monitor how well the cluster is performing, based on latency, IOPS, and throughput. The metrics are graphed every 15 seconds by hour, day, week, month, or year.
- **Network:** You can view how the network is configured with hosts and storage objects. You can view the number of ports that are available and the interfaces and storage VMs that are associated with them.

View performance on cluster dashboard

Use the dashboard to make informed decisions about workloads you might want to add or move. You can also look at peak usage times to plan for potential changes.

The performance values refresh every 3 seconds and the performance graph refreshes every 15 seconds.

Steps

1. Click **Dashboard**.
2. Under **Performance**, select the interval.

Identify hot volumes and other objects

Accelerate your cluster performance by identifying the frequently accessed volumes (hot volumes) and data (hot objects).

Steps

1. Click **Storage > Volumes**.
2. Filter the IOPS, latency, and throughput columns to view the frequently accessed volumes and data.

Monitor cluster performance using System Manager

You can monitor cluster performance by viewing information about your system on the ONTAP System Manager Dashboard.

The Dashboard displays information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

The Dashboard lets you determine the following information:

- **Health:** How healthy is the cluster?
- **Capacity:** What capacity is available on the cluster?
- **Performance:** How well is the cluster performing, based on latency, IOPS, and throughput?
- **Network:** How is the network configured with hosts and storage objects, such as ports, interfaces, and storage VMs?

In the Health and Capacity overviews, you can click  to view additional information and perform tasks.

In the Performance overview, you can view metrics based on the hour, the day, the week, the month, or the year.

In the Network overview, the number of each object in the network is displayed (for example, "8 NVMe/FC ports"). You can click on the numbers to view details about each network object.

Monitor cluster performance with Unified Manager

With Active IQ Unified Manager, you can maximize availability and maintain control of your NetApp AFF and FAS storage infrastructure for improved scalability, supportability, performance, and security.

Active IQ Unified Manager continuously monitors system health and send alerts, so your organization can free up IT staff resources. You can instantly view storage status from a single dashboard and quickly address issues through recommended actions.

Data management is simplified because you can discover, monitor, and receive notifications to proactively manage storage and quickly resolve issues. Admin efficiency is improved because you can monitor petabytes of data from a single dashboard and manage your data at scale.

With Active IQ Unified Manager, you can keep pace with fluctuating business demands, optimizing performance using performance data and advanced analytics. The reporting capabilities allow you to access

standard reports or create custom operational reports to meet the specific needs of your business.

Monitor cluster performance with Cloud Insights

NetApp Cloud Insights is a monitoring tool that gives you visibility into your complete infrastructure. With Cloud Insights, you can monitor, troubleshoot, and optimize all your resources including your public clouds and your private data centers.

Cloud Insights comes in two editions

Cloud Insights Basic Edition is designed specifically to monitor and optimize your NetApp Data Fabric assets. It provides advanced analytics for the connections between all NetApp resources including HCI and All Flash FAS (AFF) within the environment free of charge.

Cloud Insights Standard Edition focuses not only on NetApp Data Fabric-enabled infrastructure components, but also on multi-vendor and multi-cloud environments. With its enriched capabilities, you can access support for over 100 services and resources.

In today's world, with resources in play from your on-premises data centers to multiple public clouds, it's crucial to have the complete picture from the application itself to the backend disk of the storage array. The additional support for application monitoring (like Kafka, MongoDB, and Nginx) gives you the information and knowledge you need to operate at the optimal level of utilization as well as with the perfect risk buffer.

Both editions (Basic and Standard) can integrate with NetApp Active IQ Unified Manager. Customers who use Active IQ Unified Manager will be able to see join information inside the Cloud Insights user interface. Notifications posted on Active IQ Unified Manager will not be overlooked and can now be correlated to events in Cloud Insights. In other words, you get the best of both worlds.

Monitor, troubleshoot, and optimize all your resources

Cloud Insights helps you significantly reduce the time to resolve issues and prevent them from impacting end users. It also helps you reduce cloud infrastructure costs. Your exposure to insider threats is reduced by protecting your data with actionable intelligence.

Cloud Insights gives you visibility to your entire hybrid infrastructure in one place—from the public cloud to your data center. You can instantly create relevant dashboards that can be customized to your specific needs. You can also create targeted and conditional alerts that are specific and relevant to your organization's needs.

Advanced anomaly detection helps you proactively fix issues before they arise. You can view resource contention and degradation automatically to quickly restore impacted workloads. Troubleshooting goes more quickly with the automatically built hierarchy of relationships between the different components in your stack.

You can identify unused or abandoned resources across your environment, which helps you discover opportunities to right-size the infrastructure and optimize your entire spend.

Cloud Insights visualizes your system topology to gain an understanding of your Kubernetes architecture. You can monitor the health of your Kubernetes clusters, including which nodes are in trouble, and zoom in when you see a problem.

Cloud Insights helps you protect organizational data from being misused by malicious or compromised users through advanced machine learning and anomaly detection that gives you actionable intelligence on insider threats.

Cloud Insights helps you to visualize Kubernetes metrics so you can fully understand the relations between your pods, nodes, and clusters. You're able to assess the health of a cluster or a working pod, as well as the load it is currently processing—enabling you to take command of your K8S cluster and to control both the health and the cost of your deployment.

Day-to-day administration overview

The topics in this section show you how to manage your cluster with ONTAP System Manager in ONTAP 9.7 and later releases.

If you are using the ONTAP CLI to manage your cluster, see this content:

- [Cluster Expansion Express Guide](#)
- [Disks and Aggregates Power Guide](#)
- [FlexCache Volumes for Faster Data Access Power Guide](#)
- [Logical Storage Management Guide](#)
- [System Administration Reference](#)

If you are using legacy OnCommand System Manager for ONTAP 9.7 and earlier releases to manage your cluster, see the content for your ONTAP release:

- [Volume Move Express Guide](#)
- [Cluster management using System Manager 9.6 and 9.7](#)
- [Cluster management using System Manager 9.5](#)
- [Cluster management using System Manager 9.3 and 9.4](#)
- [Cluster management using System Manager 9.2 and earlier](#)

Administration overview with System Manager

ONTAP System Manager is a graphical management interface that enables you to use a web browser to manage storage systems and storage objects (such as disks, volumes, and storage tiers) and perform common management tasks related to storage systems.

Using the System Manager Dashboard, you can view at-a-glance information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

With System Manager you can perform many common tasks, such as the following:

- Create a cluster, configure a network, and set up support details for the cluster.
- Configure and manage storage objects, such as disks, local tiers, volumes, qtrees, and quotas.
- Configure protocols, such as SMB/CIFS and NFS, and provision file sharing.
- Configure protocols such as FC, FCoE, NVMe, and iSCSI for block access.
- Create and configure network components, such as subnets, broadcast domains, data and management interfaces, and interface groups.
- Set up and manage mirroring and vaulting relationships.
- Perform cluster management, storage node management, and storage virtual machine (storage VM) management operations.
- Create and configure storage VMs, manage storage objects associated with storage VMs, and manage storage VM services.

- Monitor and manage high-availability (HA) configurations in a cluster.
- Configure service processors to remotely log in, manage, monitor, and administer the node, regardless of the state of the node.

Search, filter, and sort information in System Manager

You can search for various actions and objects in System Manager. You can also search table data for specific entries.

System Manager provides two types of searching:

- [Global searching](#)

When you enter a search argument in the field at the top of each page, System Manager searches throughout the interface to find matches. You can then sort and filter the results.

- [Table-grid searching](#)

Starting with ONTAP 9.8, when you enter a search argument in the field at the top of a table grid, System Manager searches only the columns and rows of that table to find matches.

Global searching

At the top of each page in System Manager, you can use a global search field to search various objects and actions in the interface. For example, you can search for different objects by name, pages available in the navigator column (on the left side), various action items, like "Add Volume" or "Add License", and links to external help topics. You can also filter and sort the results.



For better results, perform searching, filtering, and sorting one minute after logging in and five minutes after creating, modifying, or deleting an object.

Getting search results

The search is not case-sensitive. You can enter a variety of text strings to find the page, actions, or topics you need. Up to 20 results are listed. If more results are found, you can click **Show more** to view all results. The following examples describe typical searches:

Type of search	Sample search string	Sample search results
By object name	vol_	vol_lun_dest on storage VM: svm0 (Volume) /vol/vol...est1/lun on storage VM: svm0 (LUN) svm0:vol_lun_dest1 role: Destination (Relationship)
By location in interface	volume	Add Volume (Action) Protection – Overview (Page) Recover deleted volume (Help)

Type of search	Sample search string	Sample search results
By actions	add	Add Volume (Action) Network – Overview (Page) Expand volumes and LUNs (Help)
By help content	san	Storage – Overview (Page) SAN overview (Help) Provision SAN storage for databases (Help)

Filtering search results

You can narrow the results with filters, as shown in the following examples:

Filter	Syntax	Sample search string
By object type	<type>:<objectName>	volume:vol_2
By object size	<type><size-symbol><number><units>	luns<500mb
By broken disks	“broken disk” or “unhealthy disk”	unhealthy disk
By network interface	<IP address>	172.22.108.21

Sorting search results

When you view all the search results, they are sorted alphabetically. You can sort the results by clicking

 Filter and selecting how you want to sort the results.

Table-grid searching

Starting with ONTAP 9.8, whenever System Manager displays information in a table-grid format, a search button appears at the top of the table.

When you click **Search**, a text field appears in which you can enter a search argument. System Manager searches the entire table and displays only the rows that contain text that matches your search argument.

You can use an asterisk (*) as a "wildcard" character as a substitute for characters. For example, searching for **vol*** might provide rows that contain the following:

- vol_122_D9
- vol_lun_dest1
- vol2866
- volspec1
- volum_dest_765
- volume
- volume_new4
- volume9987

Enable new features by adding license keys

Some ONTAP features are enabled by license keys. You can add license keys using ONTAP System Manager.

Steps

1. Click **Cluster > Settings**.
2. Under **License**, click →.
3. Click **Add**.

Reboot, shut down, take over, and give back nodes

You should switch a node's workload to its HA partner (takeover) before rebooting or shutting down the node.

Steps

1. Click **Cluster > Overview**.
2. Under **Nodes**, click ⚙.
3. Click the node and select the desired action.

View hardware configurations to determine problems

With ONTAP 9.8 and later, you can use System Manager to view the configuration of AFF hardware on your network and determine if problems might arise.

The hardware visualization feature enables users to quickly visualize hardware status and any potential connection issues.

ONTAP System Manager 9.8

Hardware Visualization

Tech Clip



Before you Start

For ONTAP 9.8, System Manager provides a *preview* of the capability to view AFF hardware configurations. Starting with ONTAP 9.9.1, you can view all AFF hardware configurations.

Steps

To view AFF hardware configurations, perform the following steps:

1. In System Manager, select **Cluster > Hardware**.
2. Hover your mouse over components to view status and other details.

You can view various types of information:

- [Information about controllers](#)
- [Information about disk shelves](#)
- [Information about storage switches](#)

Information about controllers

You can view the following:

Nodes:

- Rear views are displayed.
- Models with an internal disk shelf also show the disk layout in the front view.
- You can view the following platform models:

If your system is running...	Then you can view...
ONTAP 9.8	C190, A220, A300, A400, and A700
ONTAP 9.9.1	C190, A220, A250, A300, A320, A400, A700, A700s, A800, FAS500f

Ports:

- Console ports are not shown.
- A port is red if it is down.
- The status of a port and other details are shown when you hover over the port.

FRUs:

Information about FRUs appears only when the state of a FRU is non-optimal.

- Failed PSUs in nodes or chassis.
- High temperatures detected in nodes.
- Failed fans on the nodes or chassis.

Adapter cards:

- Cards with defined part number fields are shown in the slots if external cards has been inserted.
- Ports on cards are shown.
- Certain cards are shown with specific images of the cards. If the card is not in the list of supported part numbers, then a generic graphic is displayed.

Information about disk shelves

You can view the following:

Disk shelves:

- Front and rear views are displayed.
- You can view the following disk shelf models:

If your system is running...	Then you can view...
ONTAP 9.8	DS4243, DS4486, DS212C, DS2246, DS224C, and NS224
ONTAP 9.9.1	All supported disk shelf models

Shelf ports:

- Port status is displayed.
- Remote port information is shown if the port is connected.

Shelf FRUs:

- PSU failure information is shown.

Information about storage switches

- The display shows switches that act as storage switches used to connect shelves to nodes.
- Starting with 9.9.1, System Manager displays information about a switch that acts as both a storage switch and a cluster, which can also be shared between nodes of an HA pair.
- You can view the following storage switch models:

If your system is running...	Then you can view...
ONTAP 9.8	Cisco Nexus 3232C Switch
ONTAP 9.9.1	Cisco Nexus 3232C Switch Cisco Nexus 9336C-FX2 Switch

- You can view the following:
 - **Storage switch** information includes switch name, IP address, serial number, SNMP version, and system version.
 - **Storage switch port** information includes identity name, identity index, state, and other details, including remote connection.

View and submit support cases

Starting with ONTAP 9.9.1, you can view support cases from Active IQ associated with the cluster. You can also copy cluster details that you need to submit a new support case on the NetApp Support Site.



When working with ONTAP 9.9.1, to receive alerts about firmware updates, you must be registered with Active IQ Unified Manager. Refer to [Active IQ Unified Manager documentation resources](#).

Steps

1. In System Manager, select **Support**.

A list of open support cases associated with this cluster is displayed.

2. Click on the following links to perform procedures:

- **Case Number:** See details about the case.
- **Go to NetApp Support Site:** Navigate to the **My AutoSupport** page on the NetApp Support Site to view knowledge base articles or submit a new support case.
- **View My Cases:** Navigate to the **My Cases** page on the NetApp Support Site.
- **View Cluster Details:** View and copy information you will need when you submit a new case.

Manage MetroCluster sites

Starting with ONTAP 9.8, you can use System Manager as a simplified interface for managing a configuration of a MetroCluster setup.

A MetroCluster configuration allows two clusters to mirror data to each other so if one cluster goes down, the

data isn't lost.

Typically, an organization sets up the clusters in two separate geographical locations. An administrator at each location sets up a cluster and configures it. Then one of the administrators can set up the peering between the clusters so that they can share data.

The organization can also install an ONTAP Mediator in a third location. The ONTAP Mediator service monitors the status of each cluster. When one of the clusters detects that it cannot communicate with the partner cluster, it queries the monitor to determine if the error is a problem with the cluster system or with the network connection.

If the problem is with the network connection, the system administrator performs troubleshooting methods to correct the error and reconnect. If the partner cluster is down, the other cluster initiates a switchover process to control the data I/O for both clusters.

You can also perform a switchover to bring down one of the cluster systems for planned maintenance. The partner cluster handles all data I/O operations for both clusters until you bring up the cluster on which you performed maintenance and perform a switchback operation.

You can manage the following operations:

- [Set up an IP MetroCluster site](#)
- [Set up IP MetroCluster peering](#)
- [Configure an IP MetroCluster site](#)
- [Perform IP MetroCluster switchover and switchback](#)
- [Troubleshoot problems with IP MetroCluster configurations](#)
- [Upgrade ONTAP on MetroCluster clusters](#)

Set up an IP MetroCluster site

Starting with ONTAP 9.8, you can use System Manager to set up an IP configuration of a MetroCluster site.

A MetroCluster site consists of two clusters. Typically, the clusters are located in different geographical locations.

Before you start

- Your system should already be installed and cabled according to the [Installation and Setup Instructions](#) that came with the system.
- Cluster network interfaces should be configured on each node of each cluster for intra-cluster communication.



Assign a node-management IP address

Windows System

You should connect your Windows computer to the same subnet as the controllers. This will automatically assign a node-management IP address to your system.

Steps

1. From the Windows system, open the **Network** drive to discover the nodes.
2. Double-click the node to launch the cluster setup wizard.

Other systems

You should configure the node-management IP address for one of the nodes in your cluster. You can use this node-management IP address to launch the cluster set up wizard.

See [Creating the cluster on the first node](#) for information about assigning a node-management IP address.

Initialize and configure the cluster

You initialize the cluster by setting an administrative password for the cluster and setting up the cluster management and node management networks. You can also configure services like a DNS server to resolve host names and an NTP server to synchronize time.

Steps

1. On a web browser, enter the node-management IP address that you have configured: "https://node-management-IP"

System Manager automatically discovers the remaining nodes in the cluster.

2. In the **Initialize Storage System** window, perform the following:
 - a. Enter cluster management network configuration data.
 - b. Enter Node management IP addresses for all the nodes.
 - c. Provide domain name servers (DNS) details.
 - d. In the **Other** section, select the check box labeled **Use time service (NTP)** to add the time servers.

When you click **Submit**, wait for the cluster to be created and configured. Then, a validation process occurs.

What's Next?

After both clusters have been set up, initialized, and configured, perform the following procedure:

- [Set up IP MetroCluster peering](#)

Set up IP MetroCluster peering

Starting with ONTAP 9.8, you can manage an IP configuration of a MetroCluster operation with System Manager. After setting up two clusters, you set up peering between them.

Before you start

You should have completed the following procedure to set up two clusters:

- [Set up an IP MetroCluster site](#)

Certain steps of this process are performed by different system administrators located at the geographical sites of each cluster. For the purposes of explaining this process, the clusters are called "Site A cluster" and "Site B cluster".

Performing the peering process from Site A

This process is performed by a system administrator at Site A.

Steps

1. Log in to Site A cluster.
2. In System Manager, select **Dashboard** from the left navigation column to display the cluster overview.

The dashboard shows the details for this cluster (Site A). In the **MetroCluster** section, Site A cluster is shown on the left.

3. Click **Attach Partner Cluster**.
4. Enter the details of the network interfaces that allow the nodes in Site A cluster to communicate with the nodes in Site B cluster.
5. Click **Save and Continue**.
6. On the **Attach Partner Cluster** window, select **I do not have a passphrase**, which lets you generate a passphrase.
7. Copy the generated passphrase and share it with the system administrator at Site B.
8. Select **Close**.

Performing the peering process from Site B

This process is performed by a system administrator at Site B.

Steps

1. Log in to Site B cluster.
2. In System Manager, select **Dashboard** to display the cluster overview.

The dashboard shows the details for this cluster (Site B). In the MetroCluster section, Site B cluster is shown on the left.

3. Click **Attach Partner Cluster** to start the peering process.
4. Enter the details of the network interfaces that allow the nodes in Site B cluster to communicate with the nodes in Site A cluster.
5. Click **Save and Continue**.
6. On the **Attach Partner Cluster** window, select **I have a passphrase**, which lets you enter the passphrase that you received from the system administrator at Site A.
7. Select **Peer** to complete the peering process.

What's next?

After the peering process is successfully completed, you configure the clusters. See [Configure an IP MetroCluster site](#).

Configure an IP MetroCluster site

Starting with ONTAP 9.8, you can manage an IP configuration of a MetroCluster operation with System Manager. After setting up two clusters and peering them, you configure each cluster.

Before you start

You should have completed the following procedures:

- [Set up an IP MetroCluster site](#)
- [Set up IP MetroCluster peering](#)

Configure the connection between clusters

Steps

1. Log in to System Manager on one of the sites, and select **Dashboard**.

In the **MetroCluster** section, the graphic shows the two clusters that you set up and peered for the MetroCluster sites. The cluster you are working from (local cluster) is shown on the left.

2. Click **Configure MetroCluster**. From this window, you can perform the following tasks:
 - a. The nodes for each cluster in the MetroCluster configuration are shown. Use the drop-down lists to select which nodes in the local cluster will be disaster recovery partners with which nodes in the remote cluster.
 - b. Click the check box if you want to configure an ONTAP Mediator service. See [Configure the ONTAP Mediator service](#).

c. If both clusters have a license to enable encryption, the **Encryption** section is displayed.

To enable encryption, enter a passphrase.

1. Click **Save** to configure the MetroCluster sites.

On the **Dashboard**, in the **MetroCluster** section, the graphic shows a check mark on the link between the two clusters, indicating a healthy connection.

Configure the ONTAP Mediator service

The ONTAP Mediator service is typically installed at a geographic location separate from either location of the clusters. The clusters communicate regularly with the service to indicate that they are up and running. If one of the clusters in the MetroCluster configuration detects that the communication with its partner cluster is down, it checks with the ONTAP Mediator to determine if the partner cluster itself is down.

Before you start

Both clusters at the MetroCluster sites should be up and peered.

Steps

1. In System Manager 9.8, select **Cluster > Settings**.
2. In the **Mediator** section, click .
3. On the **Configure Mediator** window, click **Add+**.
4. Enter the configuration details for the ONTAP Mediator.

Perform IP MetroCluster switchover and switchback

You can switch over control from one IP MetroCluster site to the other to perform maintenance or recover from an issue.



Switchover and switchback procedures are supported only for IP MetroCluster configurations.

Overview of switchover and switchback

A switchover can occur in two instances:

- **A planned switchover**

This switchover is initiated by a system administrator using System Manager. The planned switchover allows a system administrator of a local cluster to switch control so that the data services of the remote cluster are handled by the local cluster. Then, a system administrator at the remote cluster location can perform maintenance on the remote cluster.

- **An unplanned switchover**

In some cases, when a MetroCluster cluster goes down or the connections between the clusters are down, ONTAP will automatically initiate a switchover procedure so that the cluster that is still running handles the data handling responsibilities of the down cluster.

At other times, when ONTAP cannot determine the status of one of the clusters, the system administrator

of the site that is working initiates the switchover procedure to take control of the data handling responsibilities of the other site.

For any type of switchover procedure, the data servicing capability is returned to the cluster by using a *switchback* process.

You perform different switchover and switchback processes for ONTAP 9.7 and 9.8:

- [Use System Manager 9.7 for switchover and switchback](#)
- [Use System Manager 9.8 for switchover and switchback](#)

Use System Manager 9.7 for switchover and switchback

Steps

1. Log in to System Manager 9.7.
2. Click **(Return to classic version)**.
3. Click **Configuration > MetroCluster**.

System Manager verifies whether a negotiated switchover is possible.

4. Perform one of the following substeps when the validation process has completed:
 - a. If validation fails, but Site B is up, then an error has occurred. For example, there might be a problem with a subsystem, or NVRAM mirroring might not be synchronized.
 - i. Fix the issue that is causing the error, click **Close**, and then start again at Step 2.
 - ii. Halt the Site B nodes, click **Close**, and then perform the steps in [Performing an unplanned switchover](#).
 - b. If validation fails, and Site B is down, then most likely there is a connection problem. Verify that Site B is really down, then perform the steps in [Performing an unplanned switchover](#).
5. Click **Switchover from Site B to Site A** to initiate the switchover process.
6. Click **Switch to the new experience**.

Use System Manager 9.8 for switchover and switchback

Perform a planned switchover (ONTAP 9.8)

Steps

1. Log in to System Manager 9.8.
2. Select **Dashboard**. In the **MetroCluster** section, the two clusters are shown with a connection.
3. In the local cluster (shown on the left), click , and select **Take control of remote site**.

After the switchover request is validated, control is transferred from the remote site to the local site, which performs data service requests for both clusters.

The remote cluster reboots, but the storage components are not active, and the cluster does not service data requests. It is now available for planned maintenance.



The remote cluster should not be used for data servicing until you perform a switchback.

Perform an unplanned switchover (ONTAP 9.8)

An unplanned switchover might be initiated automatically by ONTAP. If ONTAP cannot determine if a switchback is needed, the system administrator of the MetroCluster site that is still running initiates the switchover with the following steps:

Steps

1. Log in to System Manager 9.8.
2. Select **Dashboard**.

In the **MetroCluster** section, the connection between the two clusters is shown with an "X" on it, meaning a connection cannot be detected. Either the connections or the cluster is down.

3. In the local cluster (shown on the left), click , and select **Take control of remote site**.

After the switchover request is validated, control is transferred from the remote site to the local site, which performs data service requests for both clusters.

The cluster must be repaired before it is brought online again.



After the remote cluster is brought online again, it should not be used for data servicing until you perform a switchback.

Perform a switchback (ONTAP 9.8)

Before you start

Whether the remote cluster was down due to planned maintenance or due to a disaster, it should now be up and running and waiting for the switchback.

Steps

1. On the local cluster, log in to System Manager 9.8.
2. Select **Dashboard**.

In the **MetroCluster** section, the two clusters are shown.

3. In the local cluster (shown on the left), click , and select **Take back control**.

The data is *healed* first, to ensure data is synchronized and mirrored between both clusters.

4. When the data healing is complete, click , and select **Initiate switchback**.

When the switchback is complete, both clusters are active and servicing data requests. Also, the data is being mirrored and synchronized between the clusters.

Troubleshoot problems with IP MetroCluster configurations

Starting with ONTAP 9.8, System Manager monitors the health of IP MetroCluster configurations and helps you identify and correct problems that might occur.

Overview of the MetroCluster Health Check

System Manager periodically checks the health of your IP MetroCluster configuration. When you view the MetroCluster section in the Dashboard, usually the message is "MetroCluster systems are healthy."

However, when a problem occurs, the message will show the number of events. You can click on that message and view the results of the health check for the following components:

- Node
- Network Interface
- Tier (Storage)
- Cluster
- Connection
- Volume
- Configuration Replication

The **Status** column identifies which components have problems, and the **Details** column suggests how to correct the problem.

MetroCluster troubleshooting

Steps

1. In System Manager, select **Dashboard**.
2. In the **MetroCluster** section, notice the message.
 - a. If the message indicates that your MetroCluster configuration is healthy, and the connections between the clusters and the ONTAP Mediator are healthy (shown with check marks), then you have no problems to correct.
 - b. If the message lists the number of events, or the connections have gone down (shown with an "X"), then continue to the next step.
3. Click the message that shows the number of events.

The MetroCluster Health Report displays.

4. Troubleshoot the problems that appear in the report using the suggestions in the **Details** column.
5. When all the problems have been corrected, click **Check MetroCluster Health**.



The MetroCluster Health Check uses an intensive amount of resources, so it is recommended that you perform all your troubleshooting tasks before running the check.

The MetroCluster Health Check runs in the background. You can work on other tasks while you wait for it to finish.

Clone volumes and LUNs for testing

You can clone volumes and LUNs to create temporary, writable copies for testing. The clones reflect the current, point-in-time state of the data. You can also use clones to give additional users access to data without giving them access to production data.



The FlexClone license should be installed on the storage system.

Cloning a volume

Create a clone of a volume, as follows:

Steps

1. Click **Storage > Volumes**.
2. Click next to the name of the volume you want to clone.
3. Select **Clone** from the list.
4. Specify a name for the clone and complete the other selections.
5. Click **Clone** and verify that the volume clone appears in the list of volumes.

Alternatively, you can clone a volume from the **Overview** that displays when you view volume details.

Cloning a LUN

Create a clone of a LUN, as follows:

Steps

1. Click **Storage > LUNs**.
2. Click next to the name of the LUN you want to clone.
3. Select **Clone** from the list.
4. Specify a name for the clone and complete the other selections.
5. Click **Clone** and verify that the LUN clone appears in the list of LUNs.

Alternatively, you can clone a LUN from the **Overview** that displays when you view LUN details.

When you create a LUN clone, System Manager automatically enables the deletion of the clone when space is needed.

Modify QoS

Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process. You can also modify QoS after your storage has been provisioned.

Steps

1. In ONTAP System Manager, click **Storage** and select **Volumes**.
2. Next to the volume for which you want to modify QoS, click and select **Edit**.

Update firmware

You can apply a firmware update to supported devices in your cluster, such as disks, disk shelves, the Disk Qualification Package (DQP) the service processor (SP), or the Baseboard Management Controller (BMC).

Starting with ONTAP 9.9.1, you can receive alerts from Active IQ that inform you when firmware updates are pending on the cluster. Then, you can download the firmware image and upload it using System Manager.



* Starting with
ONTAP 9.9.1

View firmware update alerts from Active IQ

Starting with ONTAP 9.9.1, you can receive alerts from Active IQ Unified Manager that inform you when firmware updates are pending on the cluster.



When working with ONTAP 9.9.1, to receive alerts about firmware updates, you must be registered with Active IQ Unified Manager. Refer to [Active IQ Unified Manager documentation resources](#).

Steps

1. Go to **Dashboard**.

In the **Health** section, a message displays if there are any recommended firmware updates for the cluster.

2. Click on the alert message.

The **Firmware Update** tab is displayed in the **Update** page.

Download the cluster firmware



For ONTAP 9.8, you must navigate to the NetApp Support Site to download an updated firmware image package.

Starting with ONTAP 9.9.1, you can download firmware updates from the **Update** page when you view firmware alerts (see [View firmware update alerts from Active IQ](#)).

Steps

Perform the procedure that is appropriate for the version of ONTAP that is installed on the cluster.

For ONTAP 9.8 and ONTAP 9.9.1, if you are not registered with Active IQ Unified Manager, then perform these steps...	Starting with ONTAP 9.9.1, if you are registered with Active IQ Unified Manager, then perform these steps...
<ol style="list-style-type: none"> 1. Navigate to the NetApp Support Site. 2. Log into the NetApp Support Site. 3. Select the firmware package that you want to use to update your cluster firmware. 4. Copy the files to an HTTP or FTP server on your network or to a local folder. 	<ol style="list-style-type: none"> 1. On the Update page, for the firmware update that you want to perform, click on the link that says *Download from NetApp Support Site*. The NetApp Support Site is displayed. 2. Log into the NetApp Support Site. 3. Download the firmware image package you want to update with. 4. Copy the files to an HTTP or FTP server on your network or to a local folder.

Update the cluster firmware

After the firmware package files are downloaded, you can update the cluster firmware.

Steps

1. In ONTAP System Manager, click **Cluster > Overview**.
2. In the right corner of the **Overview** pane, click  and select **ONTAP Update**.
3. Click **Firmware Update**, select **From Server** or **Local Client** and provide the server URL or the file location.

You can monitor or verify the update under **Firmware Update Summary**.

Manage storage

Capacity measurements in System Manager

System capacity can be measured as physical space or logical space. Recent versions of System Manager use measurements of logical capacity.

The differences between the two measurements are explained in the following descriptions:

- **Physical capacity:** Physical space refers to the physical blocks of storage used in the volume. The value for physical used capacity is typically smaller than the value for logical used capacity due to the reduction of data from storage efficiency features (such as deduplication and compression).
- **Logical capacity:** Logical space refers to the usable space (the logical blocks) in a volume. Logical space refers to how theoretical space can be used, without accounting for results of deduplication or compression. The value for logical space used is derived from the amount of physical space used plus the savings from storage efficiency features (such as deduplication and compression) that have been configured. This measurement often appears larger than the physical used capacity because it includes Snapshot copies, clones, and other components, and it does not reflect the data compression and other reductions in the physical space. Thus, the total logical capacity could be higher than the provisioned space.



In System Manager, capacity representations do not account for root storage tier (aggregate) capacities.

Measurements of used capacity

Measurements of used capacity are displayed differently depending on the version of System Manager you are using, as explained in the following table:

Version of System Manager	Term used for capacity	Type of capacity referred to
9.5 and 9.6 (Classic view)	Used	Physical space used
9.7 and 9.8	Used	Logical space used (if storage efficiency settings have been enabled)
9.9.1	Logical Used	Logical space used (if storage efficiency settings have been enabled)

Measurement terms

- **Physical used:** Displays the amount of capacity used in the physical blocks of a volume.
- **Physical used %:** Displays the percentage of capacity used in the physical blocks of a volume compared to the provisioned size.
- **Logical used:** Displays the amount of used space without considering the space saved by storage efficiency features.
- **Logical used %:** Displays the percentage of the current logical used capacity compared to the provisioned size, excluding the Snapshot reserve of the volume. This value can be greater than 100%, because it includes efficiency savings in the volume.

Additional references:

"Logical space reporting and enforcement for volumes" topic in the [ONTAP 9 Logical Storage Management Guide](#)

Expand storage

You can increase the size of your volume or LUN so that more space is available to your host. The size of a LUN cannot exceed the size of the containing volume.

- [Increase the size of a volume](#)
- [Increase the size of a LUN](#)

Also, you can add a LUN to an existing volume. The processes are different for using System Manager with ONTAP 9.7 or 9.8

- [Add a LUN to an existing volume \(ONTAP 9.7\)](#)
- [Add a LUN to an existing volume \(ONTAP 9.8\)](#)

Also, starting with ONTAP 9.8, you can use System Manager to add a LUN to an existing volume.

Increase the size of a volume

Steps

1. Click **Storage > Volumes**.
2. Hover over the name of the volume you want to increase in size.
3. Click .
4. Select **Edit**.
5. Increase the capacity value.

Increase the size of a LUN

Steps

1. Click **Storage > LUNs**.
2. Hover over the name of the LUN you want to increase in size.
3. Click .
4. Select **Edit**.
5. Increase the capacity value.

Add a LUN to an existing volume (ONTAP 9.7)

To use System Manager with ONTAP 9.7 to add a LUN to an existing volume, you should switch to the Classical View first.

Steps

1. Log in to System Manager in ONTAP 9.7.
2. Click **Classical View**.
3. Select **Storage > LUNs > Create**
4. Specify the details to create the LUN.
5. Specify to which existing volume or qtree the LUN should be added.

Add a LUN to an existing volume (ONTAP 9.8)

Starting with ONTAP 9.8, you can use System Manager to add a LUN to an existing volume that already has at least one LUN.

Steps

1. Click **Storage > LUNs**.
2. Click **Add+**.
3. Complete the fields in the **Add LUNs** window.
4. Select **More Options**.
5. Select the checkbox labeled **Group with related LUNs**.
6. In the drop-down field, select a LUN that exists on the volume to which you want to add another LUN.
7. Complete the rest of the fields. For **Host Mapping**, click one of the radio buttons:
 - **Existing initiator group** lets you select an existing group from a list.

- **New initiator group** lets you enter a new group in the field.

Add disks to a local tier (Add capacity to aggregate)

You can increase the size of an existing aggregate (local tier) by adding capacity disks.

Steps

1. Click **(Return to classic version)**.
2. Click **Hardware and Diagnostics > Aggregates**.
3. Select the aggregate to which you want to add capacity disks, and then click **Actions > Add Capacity**.

You should add disks that are of the same size as the other disks in the aggregate.

4. Click **Switch to the new experience**.
5. Click **Storage > Tiers** to verify the size of the new aggregate.

Add nodes to cluster

You can increase the size and capabilities of your cluster by adding new nodes.

Before you Start

You should have already cabled the new nodes to the cluster.

There are separate processes for working with System Manager in ONTAP 9.7 or ONTAP 9.8.

- [Adding nodes to a cluster with System Manager 9.7](#)
- [Adding nodes to a cluster with System Manager 9.8](#)

Adding nodes to a cluster with System Manager 9.7

Steps

1. Click **(Return to classic version)**.
2. Click **Configurations > Cluster Expansion**.

System Manager automatically discovers the new nodes.

3. Click **Switch to the new experience**.
4. Click **Cluster > Overview** to view the new nodes.

Adding nodes to a cluster with System Manager 9.8

Steps

1. Select **Cluster > Overview**.

The new controllers are shown as nodes connected to the cluster network but are not in the cluster.

2. Click **Add**.
 - The nodes are added into the cluster.
 - Storage is allocated implicitly.

Manage storage efficiency policies

Starting with ONTAP 9.8, you can use System Manager to enable, disable, add, edit, or delete efficiency policies for storage VMs on FAS systems.



This function is not available on AFF systems.

Steps

1. Select **Storage > Storage VMs**
2. Select the storage VM for which you want to manage efficiency policies.
3. On the **Settings** tab, select → in the **Efficiency Policy** section. The efficiency policies for that storage VM are displayed.

You can perform the following tasks:

- **Enable or disable** an efficiency policy by clicking the toggle button in the Status column.
- **Add** an efficiency policy by clicking on **Add+**.
- **Edit** an efficiency policy by clicking on ⚙ to the right of the policy name and selecting **Edit**.
- **Delete** an efficiency policy by clicking on ⚙ to the right of the policy name and selecting **Delete**.

Recover deleted volumes

If you have accidentally deleted one or more FlexVol volumes, you can recover these volumes. Starting in System Manager 9.8, you can also recover FlexGroup volumes. You can also delete the volumes permanently by purging the volumes.

The volume retention time can be set on a storage VM level. By default, the volume retention time is set to 12 hours.

Selecting deleted volumes

Steps

1. Click **Storage > Volumes**.
2. Click **More > Show Deleted Volumes**.
3. Select the volumes and click the desired action to recover or permanently delete the volumes.

Resetting the volume configurations

Deleting a volume deletes the associated configurations of the volume. Recovering a volume does not reset all the configurations. Perform the following tasks manually after recovering a volume to bring the volume back to its original state:

Steps

1. Rename the volume.
2. Set up a junction path (NAS).
3. Create mappings for LUNs in the volume (SAN).
4. Associate a Snapshot policy and export policy with the volume.

5. Add new quota policy rules for the volume.

6. Add a QOS policy for the volume.

Save storage space using compression, compaction, and deduplication

For volumes on non-AFF clusters, you can run deduplication, data compression, and data compaction together or independently to achieve optimal space savings.

- Deduplication eliminates duplicate data blocks.
- Data compression compresses the data blocks to reduce the amount of physical storage that is required.
- Data compaction stores more data in less space to increase storage efficiency.



These tasks are supported for volumes on non-AFF clusters. Beginning with ONTAP 9.2, all inline storage efficiency features, such as inline deduplication and inline compression, are enabled by default on AFF volumes.

Steps

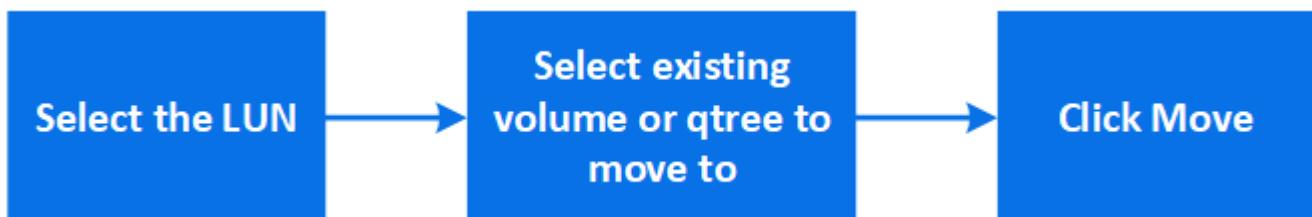
1. Click **Storage > Volumes**.
2. Next to the name of the volume for which you want to save storage, click .
3. Click **Edit** and scroll to **Storage Efficiency**.
4. *Optional:* If you want to enable background deduplication, ensure the checkbox is checked.
5. *Optional:* If you want to enable background compression, specify the storage efficiency policy and ensure the checkbox is checked.
6. *Optional:* If you want to enable inline compression, ensure the checkbox is checked.

Balance loads by moving LUNs

You can move a LUN to another volume within the storage VM to balance the load, or you can move it to a volume with a higher performance service level to improve performance.

Move restrictions

- A LUN cannot be moved to a qtree within the same volume.
- A LUN created from a file using the CLI cannot be moved with System Manager.
- LUNs that are online and serving data cannot be moved.
- LUNs cannot be moved if the allocated space in the destination volume cannot contain the LUN (even if autogrow is enabled on the volume).
- LUNs on SnapLock volumes cannot be moved with System Manager.



Steps

1. Click **Storage > LUNs**.
2. Select the LUN that you want to move and click **Move**.
3. Select an existing volume to which you want to move the LUN. If the volume contains qtrees, select the qtree.



While the Move operation is in progress, the LUN is displayed on both the origin and destination volume.

Balance loads by moving volumes to another tier

Starting with ONTAP 9.8, you can use System Manager to move a volume to another tier to balance the load.

Starting with ONTAP 9.9.1, you can also move volumes based on analysis of active and inactive data storage. For more information, see [File System Analytics overview](#).

Steps

1. Click **Storage > Volumes**.
2. Select the volume or volumes that you want to move, and then click **Move**.
3. Select an existing tier (aggregate) to which you want to move the volume or volumes.

Use Ansible Playbooks to add or edit volumes or LUNs

Starting with ONTAP 9.9.1, you can use Ansible Playbooks with System Manager when you want to add or edit volumes or LUNs.

This feature lets you use the same configuration multiple times or use the same configuration with slight changes when you add or edit volumes or LUNs.

Enable or disable Ansible Playbooks

You can enable or disable the use of Ansible Playbooks with System Manager.

Steps

1. In System Manager, go to the UI settings in the cluster settings page:
Cluster > Settings
2. Under **UI Settings**, change the slider switch to "Enabled" or "Disabled".

Save a volume configuration to an Ansible Playbook

When you create or modify the configuration of a volume, you can save the configuration as Ansible Playbook files.

Steps

1. Add or Edit the volume:

Volume > Add (or Volume > Edit)

- Specify or edit the configuration values of the volume.
- Select **Save to Ansible Playbook** to save the configuration to Ansible Playbook files.

A zip file is downloaded that contains the following files:

- **variable.yaml**: The values you entered or modified to add or edit the volume.
- **volumeAdd.yaml** (or **volumeEdit.yaml**): The test cases that are required to create or modify the values when reading the inputs from the **variable.yaml** file.

Save a LUN configuration to an Ansible Playbook

When you create or modify the configuration of a LUN, you can save the configuration as Ansible Playbook files.

Steps

- Add or Edit the LUN:

LUN > Add (or LUN > Edit)

- Specify or edit the configuration values of the LUN.
- Select **Save to Ansible Playbook** to save the configuration to Ansible Playbook files:

A zip file is downloaded that contains the following files:

- **variable.yaml**: The values you entered or modified to add or edit the LUN.
- **lunAdd.yaml** (or **lunEdit.yaml**): The test cases that are required to create or modify the values when reading the inputs from the **variable.yaml** file.

Download Ansible Playbook files from global search results

You can download Ansible Playbook files when you do a global search.

Steps

- In the search field, enter “volume” or “LUN” or “Playbook”.
- Find the search result, either “Volume Management (Ansible Playbook)” or “LUN Management (Ansible Playbook)”.
- Click on  to download the Ansible Playbook files.

Work with Ansible Playbook files

Ansible Playbook files can be modified and run to specify configurations for volumes and LUNs.

About this task

You use two files to perform an operation (either an “add” or an “edit”):

If you want to...	Use this variable file...	And use this run file...
Add a volume	volumeAdd-variable.yaml	valueAdd.yaml
Edit a volume	volumeEdit-variable.yaml	volumeEdit.yaml

If you want to...	Use this variable file...	And use this run file...
Add a LUN	<code>lunAdd-variable.yaml</code>	<code>lunAdd.yaml</code>
Edit a LUN	<code>lunEdit-variable.yaml</code>	<code>lunEdit.yaml</code>

Steps

1. Modify the variables file.

The file contains the various values that you use to configure the volume or LUN.

- If you do not change the values, leave them commented.
- If you modify the values, remove the commenting.

2. Run the associated run file.

The run file contains the test cases that are required to create or modify the values when reading the inputs from the variable file.

3. Enter your user login credentials.

Rest API

REST API log overview

The REST API log captures the API calls that System Manager issues to ONTAP. You can use the log to understand the nature and sequence of the calls needed to perform the various ONTAP administrative tasks.

How System Manager uses the REST API and API log

There are several ways that REST API calls are issued by System Manager to ONTAP.

When does System Manager issue API calls

Here are the most important examples of when System Manager issues ONTAP REST API calls.

Automatic page refresh

System Manager automatically issues API calls in the background to refresh the displayed information, such as on the dashboard page.

Display action by user

One or more API calls are issued when you display a specific storage resource or a collection of resources from the System Manager UI.

Update action by user

An API call is issued when you add, modify, or delete an ONTAP resource from the System Manager UI.

Reissuing an API call

You can also manually reissue an API call by clicking a log entry. This displays the raw JSON output from the call.

Where to find more information

- [ONTAP 9 REST API Developers Guide](#)
- [ONTAP REST API](#)

Accessing the REST API log

You can access the log containing a record of the ONTAP REST API calls made by System Manager. When displaying the log, you can also reissue API calls and review the output.

Steps

1. At the top of the page, click  to display the REST API log.

The most recent entries are displayed at the bottom of the page.

2. On the left, click **DASHBOARD** and observe the new entries being created for the API calls issued to refresh the page.
3. Click **STORAGE** and then click **Qtrees**.

This causes System Manager to issue a specific API call to retrieve a list of the Qtrees.

4. Locate the log entry describing the API call which has the form:

```
GET /api/storage/qtrees
```

You will see additional HTTP query parameters included with the entry, such as `max_records`.

5. Click the log entry to reissue the GET API call and display the raw JSON output.

Example

```
1  {
2      "records": [
3          {
4              "svm": {
5                  "uuid": "19507946-e801-11e9-b984-00a0986ab770",
6                  "name": "SMQA",
7                  "_links": {
8                      "self": {
9                          "href": "/api/svm/svms/19507946-e801-11e9-b984-
00a0986ab770"
10                     }
11                 }
12             },
13             "volume": {
14                 "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
15                 "name": "vol_vol_test2_dest_dest",
16                 "_links": {
17                     "self": {
18                         "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
00a0986abd71"
19                     }
20                 }
21             },
22             "id": 1,
23             "name": "test2",
24             "security_style": "mixed",
25             "unix_permissions": 777,
26             "export_policy": {
27                 "name": "default",
28                 "id": 12884901889,
```

```
29         "_links": {
30             "self": {
31                 "href": "/api/protocols/nfs/export-policies/12884901889"
32             }
33         },
34     },
35     "path": "/vol_vol_test2_dest_dest/test2",
36     "_links": {
37         "self": {
38             "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-
39             00a0986abd71/1"
40         }
41     },
42 ],
43 "num_records": 1,
44 "_links": {
45     "self": {
46         "href": "
47             "/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
48     }
49 }
```

Getting more information

You can get help and find more information through various resources, including videos, documentation, and forums.

- [NetApp TechCommTV](#) – more NetApp videos
- [ONTAP 9 Doc Center](#) – including Release Notes and documentation for previous versions of System Manager
- [ONTAP and ONTAP System Manager Documentation Resources](#) – including links to Technical Reports and Knowledgebase Articles
- [NetApp Community](#) – forums

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>

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

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

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

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

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

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.